



**The practical difficulties of applying the tort Private
International Law rules to the internet using online copyright
infringement as the primary research component**

A thesis submitted for the degree of Doctor of Philosophy in Law
24th October 2014

Mark Hyland

Supervisors:

Professor Alison Firth

Dr Francesco De Cecco

Dedication

I would like to dedicate this PhD to the four most important people in my life, namely, my parents, Dermot and Margaret Hyland, my wife, Chao Ji and our baby daughter, Margaret Emily.

Acknowledgements

To describe a PhD as a ‘long and winding road’ is probably one of the world’s greatest (and most misleading) euphemisms! Naivety leads one into the PhD process, but only sheer persistence and focus guides one to the ‘finish line’. Over the course of this demanding ‘project’, I ran up a rather large number of debts of gratitude.

First and foremost, I would like to say a very big ‘Thank You’ to my first supervisor, Professor Alison Firth for her immense support. Over the years, I came to really appreciate Professor Firth’s human warmth, sharp legal mind, and unquestioned pragmatism. A strong friendship developed between us over the course of the doctorate and it was thanks to Professor Firth’s commonsensical approach to the PhD, that I managed to stay relatively grounded (!) during the long journey! I would also like to extend my thanks to my second supervisor, Dr Francesco De Cecco for his insightful comments on my drafts and for his very judicious observations/comments on EU-related elements within my PhD. I also owe a word of thanks to my former second supervisor, Dr Orkun Akseli (now with Durham Law School), who dispensed very good advice in relation to the two ‘purest’ chapters on private international law, namely chapters 4 and 5. Sincere gratitude is also owed to Dr Ann Sinclair of Newcastle Law School for her kindness and sage advice. Thanks too to Ms Gemma Hayton for all the practical help over the years.

As regards my colleagues in Bangor Law School, I wish to express my gratitude to our Head of School, Professor Dermot Cahill, and his Deputy Head, Mr Aled Griffiths, for ensuring that my teaching load was somewhat lightened in the final phase of the thesis. This generous concession was very gratefully received! I would like to thank the following for the reason appearing in brackets immediately after their name:

Ms Tamara Bukatz (warning me of misdemeanours concerning OSCOLA and very careful proofreading of drafts); Mrs Carys Aaron (diligent proofreading); Dr Yvonne McDermott-Rees (moral support), Dr Emma Roberts (moral support and the loan of difficult to obtain textbooks in the field of Conflict of Laws), Mr Gwilym Owen (moral support and great practical advice about life in general and, more specifically, the elusive work/life balance), Dr Alison Mawhinney (moral support) and Dr Xavier Laurent (for the formatting of my thesis and for coaxing me back to the world of exercise!).

I am also very grateful to my parents, Dermot and Margaret Hyland, whose encouragement kept me going during the toughest periods of the PhD. Their frequent exhortations to complete the task I began helped to keep me single-minded and determined.

Lastly, I would like to thank my fantastic wife, Chao Ji, and our daughter, Emily-Margaret for their endless support and selfless attitude. To ensure that I could avail of maximum silence (the monastic experience!) during the final period of my PhD, they even absented themselves from the Principality so that I could remain fully focused. Your sacrifice is very much appreciated.

M Hyland
Gwynedd, Wales
Thur., 12 June 2014

Abbreviations, shortened titles and references

AC	Law Reports, Appeal Cases
AG	Advocate-General
AJCL	American Journal of Comparative Law
Alb LJ Sci & Tech	Albany Law Journal of Science & Technology
All ER	All England Law Reports
All SA	All South African Law Reports
ALR	Australian Law Reports
art, arts	article, articles
ATCSA	Anti-Terrorism, Crime and Security Act 2001
B2B	Business-to-Business
B2C	Business-to-Consumer
BCL Rev	Boston College Law Review
BDSG	Bundesdatenschutzgesetz (German Federal Data Protection Act)
BGH	Bundesgerichtshof (German for Supreme Court)
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen (German for Supreme Court Reporter for Civil Matters)
BPI	The British Recorded Music Industry; British Phonographic Industry
Brook J Int L	Brooklyn Journal of International Law
Brussels I	Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters
BskyB	British Sky Broadcasting
BT	British Telecommunications
C2C	Consumer-to-Consumer

Cal Crt App	Court of Appeal of California
Cal Rptr	California Reporter
Car & K	Carrington & Kirwan's Nisi Prius Reports
CD Cal	Central District of California
CDPA 1988	Copyright, Designs and Patents Act 1988
CEC	European Community Cases
CJEU	Court of Justice of the European Union
CL	Computer Law
CLIP	The European Max Planck Group on Conflict of Laws in Intellectual Property
CLR	Commonwealth Law Reports
CLS Rev	Computer Law & Security Review
CLSR	Computer Law and Security Report
Cm	Command Paper
CMBA	Creative and Business Media Association
CMLR	Common Market Law Reports
COB	Compliance Officer Bulletin
Colum L Rev	Columbia Law Review
Colum Sci & Tech L Rev	Columbia Science & Technology Law Review
Colum VLA JLA	Columbia (Volunteer Lawyers for the Arts) Journal of Law and the Arts
COM	European Commission documents
Comms L	Communications Law
Community Trade Mark Regulation	Council Regulation (EC) 207/2009 of 26 February 2009 on the Community trade mark
COPPA 1998	Children's Online Privacy Protection Act 1998
CP	Consultation Paper
CPR	Civil Procedure Rules
CR	Computer und Recht
CTLR	Computer and Telecommunications Law Review

CUP	Cambridge University Press
Database Directive	Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases
Data Retention Directive	Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
DEA 2010	Digital Economy Act 2010
DG	Directorate-General
DNJ	District of New Jersey
DPA 1998	Data Protection Act 1998
DPI	deep packet inspection
DuD	Datenschutz und Datensicherung
EBU	European Broadcasting Union
ECDR	European Copyright and Design Reports
ECJ	European Court of Justice
E-Commerce Directive	Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)
ECR	European Court Reports
EDI LR	Electronic Data Interchange Law Review, cont. as: Electronic Communication Law Review
edn	edition
EIPR	European Intellectual Property Review
EJCL	Electronic Journal of Comparative Law

Electron Bus Law Rep	Electronic Business Law Reports
ELR	European Law Review
EMLR	Entertainment and Media Law Reports
Emory Int'l L Rev	Emory International Law Review
Enforcement Directive	Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights
Ent LR	Entertainment Law Review
E-Privacy Directive	Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)
Eu LR	European Union Law Reporter
EWCA Civ	England & Wales Court of Appeal (Civil Division)
EWCA Crim	England & Wales Court of Appeal (Criminal Division)
EWHC	England & Wales High Court
EWPC	England & Wales Patents County Court
F Supp	Federal Supplement
FAPL	Football Association Premier League
FC, FCR	Canada Federal Court Reports
FCA	Federal Court of Australia
FCAFC	Federal Court of Australia: Full Court
Fed Cir BJ	The Federal Circuit Bar Journal
Fordham Intell Prop Media & Ent L J	Fordham Intellectual Property, Media & Entertainment Law Journal
FSR	Fleet Street Reports
Gaz Pal	Gazette du Palais

German LJ	German Law Journal
GRUR Int	Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil
HADOPI	Haute Autorité pour la Diffusion des œuvres et la Protection des droits d'auteur sur Internet
HCA	High Court of Australia
HKLRD	Hong Kong Law Reports & Digest
IAP	Internet Access Provider
ICLQ	International & Comparative Law Quarterly
ICO	Information Commissioner's Office
ICT	Information Communication Technologies
IEHC	High Court of Ireland
IESC	Supreme Court of Ireland
IFPI	International Federation of Phonographic Industries
IIC	International Review of Intellectual Property and Competition Law
IJLIT, Int J Law Info Tech	International Journal of Law and Information Technology
IL Pr	International Litigation Procedure
ILRM	Irish Law Reports Monthly
Indian JIntl L	Indian Journal of International Law
InfoSoc Directive	Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society
Int'l Rev L Computers & Tech	International Review of Law Computers & Technology
IP	Intellectual Property
IPJ	Intellectual Property Law Journal

IPQ	Intellectual Property Quarterly
IPR	Intellectual Property Reports
IPRs	Intellectual property Rights
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IR	Irish Reports
ISP	Internet Service Provider
IWF	Internet Watch Foundation
J Copyright Soc’y USA	Journal of the Copyright Society of the USA
J Marshall J Computer & Info L	John Marshall Journal of Computer & Information Law
JBL	Journal of Business Law
JILT	Journal of Information, Law, and Technology
Jour PIL	Journal of Private International Law
JW	Juristische Wochenschrift
LG	Landgericht (German for regional court)
Lloyd’s Rep	Lloyd’s Law Reports
LR QB	Law Reports, Queen’s Bench
M & W	Meeson & Welshby’s Exchequer Reports
Media L Rep	Media Law Reporter
ND Cal	Northern District of California
NILR	Netherlands International Law Review
NJ	New Jersey
NJW	Neue Juristische Wochenschrift
NPO	Norwich Pharmacal Order
OECD	Organisation for Economic Co-operation and development
OFCOM	Office of Communications
OJ	Official Journal
OR	Ontario Reports
OVG	Oberverwaltungsgericht (German for Higher Administrative Court)

P2P file sharing	Peer-to-peer file sharing
PDA	Personal Digital Assistant
PII	personally identifiable information
PIL	Private International Law
PIPEDA (SC 2000, c 5)	Personal Information Protection and Electronic Documents Act (SC 2000, c 5)
PwC	PricewaterhouseCoopers
Revenue LJ	Revenue Law Journal
RIPA 2000	Regulation of Investigatory Powers Act 2000
Rome I	Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations
Rome II	Regulation (EC) 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations
RPC	Reports of Patent, Design and Trade Mark Cases
Santa Clara Comp & Tech LJ	Santa Clara Computer & Technology Law Journal
SatCab Directive	Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable
SCLR	Scottish Civil Law Reports
SCR	Supreme Court Reports, Canada
SDNY	Southern District of New York
SGAE	Sociedad General de Autores y Editores de España
SGDC	Singapore District Court
SGHC	Singapore High Court

SI	Statutory Instrument
SLT (Sh Ct)	Scots Law Times, Sheriff Court Reports
t/a	Trading as
TCP	Transmission Control Protocol
TEC	Treaty Establishing the European Community
Telco (pl.: Telcos)	Telecommunications company
Texas Intl LJ	Texas International Law Journal
TFEU	Treaty of the Functioning of the European Union
TGI	Tribunal de Grande Instance
TLR	Times Law Reports
	Tulane Law Review
TPM	technological protection measure
Trade Marks Directive	Council Directive 89/104/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
UCLR	University of Chicago Law Review
UEFA	Union of European Football Association
UEJF	French Union of Jewish Students
UKHL	United Kingdom House of Lords
UKSC	United Kingdom Supreme Court
USPQ2d	United States Patents Quarterly, Second Series
Va J Int'l L	Virginia Journal of International Law
VCAP	Voluntary Copyright Alert Programme
VGH	Verwaltungsgerichtshof (Bavarian Administrative Court)
VLR	Victorian Law Reports
VSC	Victoria Supreme Court
WCT	WIPO Copyright Treaty
WD Ky	Western District of Kentucky

WIPO

World Intellectual Property Organization

WLR

Weekly Law Reports

WTO

World Trade Organization

Yale LJ

Yale Law Journal

ZASCA

Supreme Court of Appeal of South Africa

ZPO

Zivilprozessordnung (German Code of
Civil Procedure)

General Table of Content

1. The Introduction

1 The Objective of this Thesis	21
1.1 Scope of this thesis	24
1.1.5 Focus on Civil Jurisdiction	27
1.2 Feasibility Issues	29
1.3 Has PIL’s Usefulness Been Diminished in the Digital Age?	30
1.4 The Internet and PIL - Natural Bedfellows?	30
1.5 My Research Questions	31
1.6 The Interface Between the internet and PIL – Gradually Gaining in Prominence	33
1.7 Originality of this Work	36
1.8 Methodology A Library-Based Research Study	37
1.9 Structure of Thesis	40
1.10 Summing Up	40
Nature of the Internet	42
2.1 The Internet – A network of computers and servers	43
2.2 An Open, cooperative, flexible and decentralised medium	44
2.3 Tensions between the internet and copyright	45
2.4 Border-disregarding	47
2.5 The internet in China – a four-tier system	47
2.6 Geographical independence	48
2.7 Low-threshold information distribution	48
2.8 Portability	49
2.9 Nature of the Internet (as seen from the copyright perspective)	49
2.9.1 The seamlessness of the Internet	50
2.10 Characteristics of Infringement over the Internet	51
2.10.1 Problems of identity and location of the parties	51
2.10.2 Difficulty in locating where the act of infringement occurred	51
2.10.3 Ubiquitous and multi-state Infringement	54
2.10.5 How today’s digital content landscape has been impacted by P2P	55
2.10.5 Other facets of the Internet	58
2.11 The EU’s PIL framework and its protective scheme for consumers	58

2.12	The internet – bordered or borderless?	61
2.13	Conclusions	63
3. Transnational Intellectual Property Infringement with Focus on Copyright		
3.1	The Objective of this Chapter	66
3.2	The proliferation of transborder copyright infringement	66
3.3	Essential elements needed in legal proceedings concerning copyright	69
3.4	Tensions between a deterritorialised internet and territorial IP	73
3.5	The UK	78
3.5.1	Lucasfilm Ltd v Ainsworth	78
3.6	Court of Justice of the European Union	81
3.6.1	Football Association Premier League Ltd v QC Leisure and Karen Murphy v Media Protection Services Ltd	81
3.6.2	Eva-Maria Painer v Standard VerlagsGmbH	85
3.6.3	Peter Pinckney v KDG Mediatech AG	86
3.6.4	Football Dataco Ltd v Sportradar	91
3.6.4.2	The Territoriality of the Sui Generis Right	93
3.6.4.3	Re-utilisation by means of a web server	94
3.6.4.4	Evidence of an intention to target persons in a different Member State	95
3.6.4.5	Rejection of the Emission Theory	96
3.6.4.6	Communication Theory or Emission Theory?	97
3.7	Conclusions	97
4. Private International Law - Jurisdiction		
4.1	Introduction	101
4.2	Jurisdiction	101
4.2.1	The basic rule of jurisdiction	105
4.2.2	Special jurisdictional provisions	107
4.2.3	Important case law relating to Article 5(3)	110
4.2.4	The new Article 5(3)	122
4.2.5	How will the new Article 5(3) operate in practice?	124
4.2.6	Lis Pendens	125
4.3	Conclusions	128

5. Private International Law - The Applicable Law	
5.1 Introduction	132
5.2 The Applicable Law	133
5.2.1 The Rome II Regulation	133
5.2.2 Specific Rules for Special Torts	135
5.2.3 Article 8 of Rome II and the Infringement of IPRs	135
5.3 The Berne Convention for the Protection of Literary and Artistic Works	138
5.3.1 Differing Views on the Actual Meaning of Article 5(2) of the Berne Convention	140
5.4 The Rule of Origin versus the Rule of Reception	146
5.4.1 The Satellite and Cable Directive	147
5.5 The European Commission's 1995 Green Paper on Copyright	151
5.6 Advantages Associated with the Country of Origin Rule	153
5.7 Disadvantages Associated with the Country of Origin Rule	155
5.8 Points of Attachment	157
5.9 An Alternative – The Law of the Country of Reception	159
5.10 Conclusions	161
6. Models and Analogues for Online Copyright Infringement, How Compelling is the Defamation Analogue?	
6.1 The aim of this chapter	165
6.2 Push/Pull dichotomy	166
6.3 Copyright's exclusive rights	168
6.4 The scope of my analysis in this chapter	169
6.5 Conceptual Models	171
6.6 A definition of defamation and how it evolves through the case-law	172
6.7 Online Defamation	173
6.8 Online Copyright Infringement	177
6.9 Points of connection/disconnection between online defamation and online infringement of the reproduction right	183
6.9.1 Points of Connection:	183
6.9.2 Points of Disconnection:	184
6.10 Communication to the Public	185
6.10.1 Dramatico Entertainment Limited v British Sky Broadcasting	186
6.10.2 EMI Records Limited v British Sky Broadcasting Limited	187

6.10.3	Football Association Premier League Limited v British Sky Broadcasting.....	191
6.11	Points of connection/disconnection	192
6.12	Right of making available to the public: the views of various commentators	194
6.13	Possible application of the communication theory and the emission theory	194
6.14	Where the making available right takes place according to Sterling	195
6.15	European Commission’s Localisation Criteria for the Making Available Right	197
6.16	Criterion No. 1 - Location of the servers upon which the works are hosted (step 3).....	197
6.17	Criterion No. 2 – Centre of activities of the uploader: establishment, domicile or habitual residence (no correspondence with the ‘step’ analysis) ...	198
6.17.1	The Advantage of using this criterion	199
6.17.2	Some problems arising from use of this criterion.....	200
6.18	Criterion No 3 – Where the material act of upload is initiated (Step 2).201	
6.18.1	Some problems associated with this criterion	202
6.19	Points of connection/disconnection between Sterling and the European Commission Study on the making available right	202
6.19.1	Points of connection	202
6.19.2	Points of disconnection	203
6.20	Conclusions.....	203
6.20.1	Reproduction right versus Defamation.....	203
6.20.2	Online Communication to the public versus online defamation	204
6.20.3	The Making Available Right.....	205
7.	Jurisdictional Issues, Article 2, Brussels 1 - Facilitative Elements	
7.1	Introduction.....	208
7.2	Article 2, Brussels I.....	209
7.3	The Facilitative Elements	213
7.3.1	The First Facilitative Element - Norwich Pharmacal Relief	213
7.3.2	Case law featuring Norwich Pharmacal relief.....	214
7.3.3	Digital Economy Act 2010.....	223
7.3.4	Technical Measures Legislation in France and the Republic of Ireland	224
7.3.5	Section 97A CDPA 1988 and Blocking of Websites	225
7.3.6	The Second Facilitative Element – Geolocation Technology	237

7.3.7	The Various Uses of Geolocation.....	238
7.3.8	Geolocation as an enforcement tool	238
7.3.9	Ensuring compliance with territorially-limited copyright laws.....	239
7.3.10	Limiting access to online content from abroad	241
7.3.11	The Accuracy of Geolocation Technology.....	241
7.3.12	Accuracy of Geolocation Technologies Impugned	245
7.3.13	The Growing Influence of Geolocation Technology in the Courts	247
7.3.14	Possible Legal Obstacles to the use of Geolocation Technology	251
7.3.15	Some Conclusions on Geolocation Technology.....	255
7.4	The Third Facilitative Element – Data Retention Legislation.....	257
7.4.1	How Directive 2006/24/EC was implemented into UK law	258
7.4.2	Data Retention (EC Directive) Regulations 2009	259
7.4.3	The communications data to be retained under the Schedule to the Regulations.....	259
7.4.4	CJEU’s ruling in Digital Rights Ireland	261
7.4.5	A Preliminary Ruling concerning the validity of Directive 2006/24/EC	261
7.4.6	The General absence of limits	263
7.4.7	The data retention period.....	263
7.4.8	Interference with the fundamental rights set out in the Charter	263
7.4.9	The rules relating to security and protection	264
7.4.10	Outcome of the case	265
7.4.11	Implications of the ruling	265
7.4.12	The Anti-Terrorism, Crime and Security Act 2001.....	267
7.5	Conclusions.....	268
8. Jurisdictional Issues, Article 2 - Brussels I - Non-Facilitative Elements		
8.1	The Objective of the Chapter.....	272
8.2	Tracing Internet Traffic	272
8.2.1	The ‘Leasing’ or Dynamic Allocation of IP Addresses	276
8.3	Conclusions.....	282
9. Jurisdictional Issues, Article 5 (3), Brussels I		
9.1	Introduction.....	285
9.2	Article 5(3), Brussels I	285
9.2.1	The New Wording of Article 5(3), Brussels I and Challenges for Conflicts Lawyers	287

9.3	Establishing the Locus of the Tort – the 2002 Dow Jones v Gutnick ruling	288
9.3.1	Dow Jones & Company Inc v Gutnick.....	288
9.3.2	Implications of the ruling	295
9.3.3	Jurisprudential inconsistency, post-Dow Jones	296
9.3.4	English rulings which followed the Gutnick Approach	297
9.3.5	The Defamation Act 2013	299
9.3.6.2.	The Ministry of Justice’s Consultation Paper.....	301
9.4.	Conclusions	301
10.	General Conclusions	303
10.1	Introduction: problems and solutions.....	304
10.2	PIL’s slow adaptation to the online world.....	304
10.3	Dow Jones v Gutnick: place of upload or place of download?	305
10.4	Proxy war for the struggle between the single publication rule and the multiple publication rule?	306
10.5	Facilitative and non-facilitative elements (viewed from the perspective of Article 2, Brussels I).....	308
10.5.1	Norwich Pharmacal relief (facilitative)	309
10.5.2	Geolocation technology (facilitative)	309
10.5.3	Data retention legislation (facilitative).....	311
10.5.4	The Dynamic Allocation of IP addresses (non-facilitative)	312
10.5.5	Facilitative elements versus non-facilitative elements	312
10.6	Models and analogues for online copyright infringement	313
10.6.1	Reproduction right versus Defamation.....	313
10.7	Research Questions and Answers.....	316
10.7.1	Question 1.....	316
10.7.2	Question 2.....	317
10.7.3	Question 3.....	318
10.7.4	Question 4.....	318
10.7.5	How well established is the lex loci protectionis within Europe?	319
10.8	Some final conclusions.....	319

CHAPTER 1. INTRODUCTION

1	The Objective of this Thesis	21
1.1	Scope of this thesis	24
1.1.5	Focus on Civil Jurisdiction.....	27
1.2	Feasibility Issues	29
1.3	Has PIL’s Usefulness Been Diminished in the Digital Age?	30
1.4	The Internet and PIL - Natural Bedfellows?	30
1.5	My Research Questions	31
1.6	The Interface Between the internet and PIL – Gradually Gaining in Prominence	33
1.7	Originality of this Work	36
1.8	Methodology A Library-Based Research Study	37
1.9	Structure of Thesis	40
1.10	Summing Up	40

1 The Objective of this Thesis

The objective of this thesis is to analyse the very real and practical difficulties faced by lawyers in applying the tort private international law (PIL) rules to the internet and to investigate which factors, technology-related or otherwise, either assist or hinder the application of the PIL rules to the internet. These practical difficulties arise from the fact that many of the basic provisions of PIL relate to physical world (or offline) elements such as domicile, nationality and place of damage or harmful event (*locus delicti*). Effective application of PIL rules is dependent on sovereign competence operating within clear jurisdictional borders. As a consequence, difficulties arise for conflicts lawyers as the internet often disregards borders. Ubiquitous torts, such as unauthorised peer-to-peer (P2P) file-sharing affecting copyright works and online defamation have become commonplace in the online world.

While geolocation technology¹ and state control of the internet² have both helped ‘erect’ borders on the internet, and aided conflicts lawyers in the process, considerable difficulty still lies in pinpointing the place of the harmful event in an online context. The localisation of the *locus delicti* is of particular importance for the application of Article 5(3) of Brussels I.³ In both online copyright and online defamation cases, there is the obvious dichotomy between place of upload and place of download. Localisation

¹ See para 7.3.6. onwards.

² See para 2.11.

³ Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1, known colloquially as Brussels I. The Brussels I Regulation has been revised by virtue of Regulation 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L351/1. While it is already in force, it will only apply to proceedings within the EU from 10 January 2015. Consequently, both the European courts and academic commentators continue to refer to Brussels I and use the article numbering of Brussels I. For this reason, I intend using and referring to Brussels I and its provisions in this thesis. Interestingly, the revised Brussels I addresses a limited number of circumstances under which Member State courts can exercise jurisdiction even if the defendant is not domiciled within the EU. In this regard, see Article 17(2) (consumer contracts) and Article 20(2) (individual contracts of employment) of revised Brussels I.

is further exacerbated by the widespread availability of portable internet-enabled devices coupled with general mobility of citizens in the 21st century.

In many respects, the challenge for conflicts lawyers is to apply rules and principles formulated for a material world to a non-material environment. This non-material environment does not comprise sovereign States or clear jurisdictional borders - the traditional 'landscape' where PIL issues are played out.⁴

In analysing the interface between PIL (or conflict of laws) and the internet, I have chosen as my primary research component, online copyright infringement. This is for two reasons. Firstly, it is arguable that it is the branch of IP Law which is subject to the greatest number of online infringements and, therefore, has been particularly affected by the dawn of the internet.⁵ Secondly, by virtue of the Berne Convention⁶ and its widespread membership, copyright comes into being almost worldwide and is not subject to a registration requirement. The internet has become a veritable battleground for copyright protection with, for example, unauthorised peer-to-peer ('P2P') file-sharing very much to the fore in the 'battle'. According to IFPI, 26 per cent of internet users worldwide regularly access illegal websites and they estimate that that figure could rise as consumers migrate to smartphone and tablet-based mobile services.⁷ In

⁴ Certain sovereign states comprise separate jurisdictions, such as the UK which comprises three separate jurisdictions, i.e. England & Wales, Scotland, and Northern Ireland. Other countries which are divided into numerous jurisdictions, each with its own distinct legal system, include the US, Canada, and Australia.

⁵ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 547 (referring generally to Jane C Ginsburg, 'Putting Cars on the Information Superhighway: Authors, Exploiters and Copyright in Cyberspace' (1995) 95 Colum L Rev 1466), where they state: 'Infringement over the internet is most likely to arise in cases of breach of copyright.'

⁶ See para 5.3 generally.

⁷ Adam Sherwin, 'Music sales fail to go in One Direction as growth turns to 3.9% decrease' (*The Independent*, 18 March 2014) <<http://www.independent.co.uk/arts-entertainment/music/news/music-sales-fail-to-go-in-one-direction-as-growth-turns-to-39-decrease-9200304.html>> accessed 21 May 2014 It is also revealing to read the attitudes of Europeans when it comes to IP. For instance, 42% of Europeans consider it acceptable to download or access copyright-protected content illegally when it is for personal use. OHIM, 'European Citizens and Intellectual Property: Perception, Awareness and Behaviour'

terms of the UK, the BPI's 'Digital Music Nation' report (2013) states that around 4 million people in the UK use both BitTorrent and P2P each month to obtain unauthorised copyright material.⁸ In the same report, there is reference to the monitoring service, MusicMetric's first 'Digital Music Index' report which estimates that over 43 million downloads were made via BitTorrent alone in just the first six months of 2012. Of those, 78% were albums and 22% single tracks, equating to 345 million tracks downloaded via BitTorrent,⁹ most of them in infringement of copyright/related rights.

When it comes to the use of illegal content, the 2013 Kantar Media report (prepared for Ofcom) claims that 35% of individuals avail of P2P technology to access illegal content. This contrasts with only 6% of individuals using P2P to access content legally.¹⁰ However, the news is not all bad for copyright owners. Website blocking measures implemented by Internet Service Providers ('ISPs') have generally been effective.¹¹ Between January 2012 and July 2013, BitTorrent use declined by 11% in European countries where blocking orders were put in place. The UK and Italy saw particularly positive results from web-blocking.¹² Sweden too has been somewhat of a poster boy for the resurgence of a recorded music market. Between 2008 and 2013, the turnover of that country's music market rose by around 27%, to Skr991million (\$155million). Spotify's launch in 2008 and a new anti-piracy law in 2009 helped nudge

(November 2013) 13 <https://oami.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/25-11-2013/european_public_opinion_study_web.pdf> accessed 21 May 2014.

⁸ BPI, 'Digital Music Nation 2013 – The UK's digital music landscape' (January 2013) 5 <www.bpi.co.uk/assets/files/BPI_Digital_Music_Nation_2013.PDF> accessed 8 May 2014.

⁹ Ibid 26.

¹⁰ Danny Kay, 'Online Copyright Infringement Tracker Wave 3 (Covering period Nov 12-Jan 13) Overview and key findings' (*Kantar Media*, 2013) 17 <<http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/w3/annexw3.pdf>> accessed 8 May 2014.

¹¹ See para 7.3.5.

¹² IFPI, 'IFPI Digital Music Report 2014 – Lighting up New Markets' (April 2014) 41 <<http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf>> accessed 8 May 2014.

many Swedes to switch from illegal downloading. Of the 3 million or so Swedes who have streaming accounts, two thirds of them are paying subscribers.¹³

Lastly, here in the UK, the government announced recently, the possible establishment of a new copyright enforcement framework for late-2014. The mooted Voluntary Copyright Alert Programme,¹⁴ involving collaboration between ISPs and rightholders, seems to be a reaction to the very delayed implementation of the Digital Economy Act 2010 (DEA).¹⁵ The proposed ‘educational letters’ under the VCAP sound suspiciously similar to the DEA’s copyright infringement reports which will not issue now until end-2015, at the earliest. The programme cannot be finalised until approval from the Information Commissioner’s Office is forthcoming.

It is important to point out at this Juncture that the scope of the copyright component of this thesis extends beyond illegal peer-to-peer activity. This fact is borne out by chapter 3 which examines transnational IP infringement (principally, copyright infringement) in more detailed terms. Aspects of transnational copyright treated in chapter 3 include artistic works (*Lucasfilm*), satellite broadcasting of audiovisual content (*Football Association Premier League v QC Leisure*), physical and digital photos (*Eva Maria Painer* ruling) and, the related *sui generis* database right (*Football Dataco v Sportradar*).

1.1 Scope of this thesis

The primary jurisdictional scope of this thesis is the UK/EU. As PIL is one of the central themes in this thesis, the EU’s sophisticated and largely harmonised PIL framework features prominently in this work. In terms of the copyright component, it too has a strong EU centre of gravity. In chapter 6, on the defamation analogue, I focus

¹³ ‘I have a stream – The land of Abba takes to streaming’ (*The Economist*, 22 March 2014) <<http://www.economist.com/news/business/21599353-land-abba-takes-streaming-i-have-stream>> accessed 21 May 2014.

¹⁴ Pinsent Mason LLP, ‘Voluntary Copyright Alert Programme could be operational before end of 2014, says UK government’ (*Out-Law*, 24 March 2014) <<http://www.out-law.com/en/articles/2014/march/voluntary-copyright-alert-programme-could-be-operational-before-end-of-2014-says-uk-government/>> accessed 21 May 2014.

¹⁵ See para 7.3.3.

on the UK and EU copyright regimes and critically evaluate the localisation of some of the key restricted rights in an online context.

Given the global and ubiquitous nature of the internet however, and the fact that online torts do not respect national borders, it is difficult to totally exclude developments (legal and otherwise) which occur outside the EU.

The principal elements in this thesis which fall outside the primary jurisdictional scope of this work are as follows:

- Geolocation technology and certain North American rulings which refer to the technology's value or usefulness
- State control and filtering of the internet (Where China and Saudi Arabia, respectively, are used as examples)
- The landmark Australian High Court ruling in the field of online defamation – *Dow Jones v Gutnick*¹⁶

I shall now justify their inclusion.

Geolocation features in this thesis because of its ability to link IP addresses to physical locations. This translates into a facility for potentially pinpointing the *locus* of an online copyright infringement committed via an internet-enabled device. While the technology's usefulness is not in doubt, its impact in Europe is still rather weak.¹⁷ This fact is highlighted by Svantesson when he criticises the CJEU's failure to consider the use of geolocation technology in joined cases *Pammer v Reederei Karl Schluter GmbH & KG, and Hotel Alpenhof GesmbH v Oliver Heller*,¹⁸ which concerned website reservations.¹⁹

¹⁶ *Dow Jones v Gutnick* [2002] HCA 56.

¹⁷ See for instance recent acquisition of an Israeli geolocation startup – Kitlocate – by the Russian internet giant Yandex. Inbal Orpaz, 'Russian Internet giant Yandex acquiring Israeli geolocation startup Kitlocate' (*Haaretz*, 18 March 2014) <<http://www.haaretz.com/business/.premium-1.580480>> accessed 21 May 2014.

¹⁸ Joined Cases C-585/08 and C-144/09 *Pammer v Reederei Karl Schlüter*; and *Hotel Alpenhof v Oliver Heller* [2010] ECR I-12527. This case is dealt with at para 2.10..

¹⁹ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 424.

To contrast judicial attitudes to the technology, I looked at the US rulings in *National Federation of the Blind v Target Corp*,²⁰ and *Hageseth v Superior Court of San Mateo County*,²¹ where the technology's value was recognised and encouraged. Nor is it just court rulings from outside the EU that are apposite. Legislators too are showing an awareness of the technology. The Australian Interactive Gambling Act 2001 (albeit through its explanatory memorandum) makes reference to the technology.

In this thesis, I have cited the works of three academic commentators who have written about the interface between geolocation technology and the law. While they are all based outside Europe, their contribution to intellectual debate on geolocation and particularly its utility as an evidential tool in court proceedings, justifies treatment of their work. The authors in question are: Svantesson of Bond University, Australia, Trimble of William S Boyd Law School, Nevada, and Kevin F King, law clerk at the US Court of Appeal for the Fourth Circuit.

King is important in that he has observed the increasing accuracy rates of the technology while Svantesson opines that the technology has achieved sufficient levels of accuracy to be used for legal purposes. While the technology's 'footprint' may still primarily be outside the EU, its endorsement by the Bavarian court (and separately by expert evidence given by Professor Thomas Hoeren) in *Bay VGH*,²² means that its impact on courts in EU Member States is beginning to grow.

China and Saudi Arabia are analysed, but in the specific context of proving how *bordered* the internet has become over the last decade.²³ These 'borders' are often coterminous with either national or possibly regional borders and are often linked to either physical manipulation of internet architecture (e.g. China's Great Firewall) or content filtering carried out within a certain national territory (e.g. Saudi Arabia's pervasive filtering system which blocks requests for blacklisted sites).

In terms of non-EU case law treated in this PhD, the High Court of Australia's *Dow Jones v Gutnick*²⁴ ruling is pre-eminent. Justification for its inclusion lies in the fact that

²⁰ *National Federation of the Blind v Target Corp*, 452 F Supp 2d 946 (ND Cal 2006).

²¹ *Hageseth v Superior Court of San Mateo County*, 150 Cal App 4th 1399.

²² VGH Bayern 20.11.2008, 10 CS 08.2399.

²³ At para 2.11.

²⁴ *Jones v Gutnick* [2002] HCA 56. This ruling is analysed from para 9.3 onwards.

it is a landmark ruling situated at the intersection between PIL and internet torts. Despite being a controversial ruling with potentially negative implications for both freedom of expression on the internet and online publication, it does establish an important rule for the localisation of online defamation, with implications therefore for both jurisdiction and choice of law. To this day, it remains the highest ruling anywhere in the world to consider the issue of jurisdiction for the purposes of publication of defamatory material on the internet. In addition, treatment of this ruling is a core element in my analysis of points of connection and points of disconnection between online copyright infringement and online defamation in chapter 6.

The important Canadian ruling of *BMG Canada Inc v John Doe*,²⁵ treated in chapter 8 is also compelling due to its careful analysis of dynamic allocation of IP addresses and its implications from an evidence viewpoint. The comprehensive reference in the ruling to the content of affidavits filed by the ISPs' employees highlights very vividly the challenges involved in linking IP addresses to actual subscribers where IP addresses are dynamically allocated. The fact that the ruling concerned both file-sharing and privacy justifies its inclusion in this PhD. At Federal Court of Appeal level, a delicate balance had to be struck between privacy interests and the public interest. This has certain parallels with the High Court ruling in *Golden Eye (International) Ltd v Telefonica*²⁶ (analysed at para 7.3.2.) where Arnold J had to strike a balance between the protection of IPRs and the fundamental rights of individuals under the EU Charter of Fundamental Rights.

1.1.5 *Focus on Civil Jurisdiction*

This thesis will only address civil aspects of the various fields of law covered by this work. There are two practical reasons for focusing on the civil aspects of copyright prosecution. Firstly, the material scope of the three principal EU PIL regulations, ie Brussels I, Rome I²⁷ and Rome II²⁸ covers 'civil and commercial matters', not

²⁵ *BMG Canada Inc v John Doe* [2004] FC 488.

²⁶ *Golden Eye (International) Ltd v Telefonica UK Ltd* [2012] EWHC 723 (Ch).

²⁷ Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6.

²⁸ Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40.

criminal matters. Secondly, criminal prosecution of copyright infringement is relatively rare²⁹ and this fact holds for most countries. While copyright infringement is normally a civil action, meaning that the copyright owner is suing the alleged infringer, it can also be a criminal act, meaning that the State brings the alleged infringer to court. However, the failure of the proposed EU Directive on criminal measures aimed at ensuring the enforcement of IPRs³⁰ and the European Parliament's rejection on 4 July 2012 of the Anti-Counterfeiting Trade Agreement (ACTA)³¹ suggest that civil rather than criminal enforcement is seen as preferable in the EU.

The focus on civil jurisdiction becomes apparent in chapter 7 through treatment of *Norwich Pharmacal* relief and similar orders available under the Enforcement Directive (Directive 2004/48/EC). Detailed consideration is given to blocking injunctions

²⁹ Louis Harms, 'The Enforcement of Intellectual Property Rights By Means of Criminal Sanctions: An Assessment' (WIPO Advisory Committee on Enforcement, WIPO/ACE/4/3, 7 September 2007) para 19, where it is stated that IPR enforcement, in principle, should be civil, and that that is the preferred method of protecting IPRs in developed countries; Lionel Bently and Brad Sherman, *Intellectual Property Law* (3rd edn, OUP 2009) 1124, where the authors state that for the most part, there has been little demand for criminal sanctions to protect IPR. This, the authors suggest, is linked to right holders' preference for the lower standard of proof associated with civil actions. Laura Gasaway, 'Criminal copyright infringement' (*Copyright Corner*, April 2004)

<<http://www.unc.edu/~uncnlg/copy-corner66.htm>> accessed 16 August 2012; Lee A Hollaar, 'Chapter 1: An Overview of Copyright' (*Digital Law Online*, 2002) I.L.4. <<http://digital-law-online.info/lpdi1.0/treatise16.html>> accessed 23 July 2010, where it is stated: 'While copyright infringement is normally a civil action, meaning that the copyright owner is suing the alleged infringer, it can also be a criminal act, meaning that the United States Government brings the alleged infringer into court.'

³⁰ The proposed Directive was officially withdrawn by way of an Official Journal notice, see European Commission, 'Withdrawal of Obsolete Commission Proposals' [2010] OJ C252/9, where there is reference to the original document – European Commission, 'Proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights' COM (2005) 276 final.

³¹ European Parliament Press Service, 'European Parliament rejects ACTA' (*European Parliament News*, 4 July 2012) <<http://www.europarl.europa.eu/news/en/pressroom/content/20120703IPR48247/html/European-Parliament-rejects-ACTA>> accessed 16 August 2012.

available under national laws,³² especially after Article 8 and Recital (59) of Directive 2001/29/EC (the InfoSoc Directive) have triggered litigation that renders the Digital Economy Act 2010 otiose.

As regards data retention laws, my principal focus will be on the recent CJEU ruling in *Digital Rights Ireland v Minister for Communications*³³ where the Data Retention Directive (Directive 2006/24/EC) was ruled invalid. Unsurprisingly, this judgment has created significant uncertainty and confusion among lawyers and academic commentators. As the UK secondary legislation transposing the Data Retention Directive is still in force, I have examined it but rather superficially, bearing in mind the recent ruling.

1.2 Feasibility Issues

To a certain extent, my analysis goes to the feasibility of applying the tort PIL rules to the internet. In the context of Brussels I, the issue of localising the harmful event is undoubtedly important. But this task is far from straightforward in an online environment and may have been significantly underestimated by drafters of EU conflicts legislation.

At least one other commentator has perceived the feasibility problems in terms of conventional application of conflict of laws doctrines to the unique characteristics of cyberspace. That same writer contends that the non-geographic character of the internet makes it very difficult to apply current, territorially-based PIL rules to activities online.³⁴

³² At para 7.3.5.

³³ Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; and Kärntner Landesregierung* (CJEU (Grand Chamber) 8 April 2014).

³⁴ Elizabeth Longworth, 'The possibilities for a legal framework for cyberspace including a New Zealand perspective' in Bruno De Padirac (ed), *The International Dimensions of Cyberspace Law (Law of Cyberspace Series, vol 1)* (Ashgate 2001) 35. This contention is bolstered by the views expressed in Lord Collins of Mapesbury et al (eds), *Dicey, Collins and Morris: The Conflict of Laws*, vol 1 (15th edn, Sweet & Maxwell 2012) 10, where it is argued that:

1.3 **Has PIL's Usefulness Been Diminished in the Digital Age?**

While the central theme of this thesis relates to the feasibility of applying the tort PIL rules to the internet, an important sub-theme emerges during the research; has the value or utility of PIL in general been diminished by the emergence of a de-territorialised internet? Given the wholly natural and close relationship (some would say, mutual dependence) between PIL and a *bordered* world, there is a very real risk that this symbiotic relationship will be weakened by the rapid emergence and growing importance of a border-disregarding internet which has become the tapestry for both torts and contractual disputes. The situation is further complicated by the incidence of ubiquitous infringement, made possible by the pervasiveness of the internet.

1.4 **The Internet and PIL - Natural Bedfellows?**

While the application of the tort PIL rules to the internet is far from problem-free, even a cursory glance at the internet's physical structure reinforces the perception that it generates tremendous scope for conflicts issues to arise. The transnational nature of the internet is demonstrated by the following: where there is no direct physical connection and peering agreement³⁵ in place between two networks, internet traffic has to find another route. Messages use the internet protocols to route around gaps or blockages. So a user in London accessing a site down the road could find that the message is routed via the US.

This could happen if the user's internet access provider is, say, a US company with an international network but no peering arrangement with another English network. The user dials into an English node of the access provider's network, but the network's gateway to the rest of the internet is in the US. The message has to go from the user to the London node, cross the access provider's network to the US, transfer to another internet-compliant US network, travel back across the Atlantic to another English

It has not been easy for the conflict of laws to adapt itself to the changes in social and commercial life which the 20th century has witnessed. Many of its rules were laid down in the 19th century and seem better suited to 19th century conditions than to those of the 20th century. By logical extension, PIL's adaptation to a border disregarding internet would be fraught with even greater difficulties!

³⁵ A peering agreement is a contractual arrangement that governs the exchange of Internet traffic between two networks.

network and thence to the target English site. The route, however, is unpredictable. So, not only is the responsibility for ensuring safe delivery of a message diffused among various networks, but the identity of those networks cannot accurately be predicted in advance.³⁶

1.5 My Research Questions

My research questions are five in number. They relate primarily to jurisdiction, but the fifth research question relates to the key choice of law rule in the field of IP Law - the *lex loci protectionis*.³⁷

1. What are the main practical difficulties that arise in terms of applying the EU tort PIL rules to the internet?
2. What role does technology play in conflicts scenarios in the twenty-first century? And, on balance, who derives greater benefit from technology - the claimant (IP owner) or the defendant (IP infringer)?
3. In terms of applying Articles 2 and 5(3), Brussels I, to an internet environment, which elements are either facilitative or non-facilitative when it comes to the *effective* application of those provisions?
4. In terms of applying Article 5(3), Brussels I, to online IP infringements, how useful is the analogue of online defamation?
5. How well established is the *lex loci protectionis* within Europe?

It is important to note that this thesis is not attempting to answer the question: whether PIL can be applied to an online environment. It goes without saying that PIL will apply to online scenarios just as it applies to offline scenarios. Rather, this thesis focuses on the practical application of certain substantive tort PIL provisions to the internet, highlighting the difficulties that arise during their application.

The interface between PIL and the internet is an obvious one, since the internet is, by its very nature and physical make-up, transnational.³⁸ This transnational character virtually

³⁶ Graham JH Smith, *Internet Law and Regulation* (4th edn, Sweet & Maxwell 2007) para 1-010.

³⁷ See para 5.2.3.

³⁸ Mireille van Eechoud, *Choice of Law in Copyright and Related Rights – Alternatives to the Lex Protectionis* (1st edn, Kluwer Law International 2003) 5, where the author states as follows:

guarantees that conflicts issues will arise since many of the legal disputes associated with the internet will involve elements from different countries.³⁹

The description of the interface as ‘complex’ is certainly justified. The interface is between a field of law designed primarily for the offline world and a medium that makes the online world possible. The confluence of these two very different rivers gives rise to choppy waters. For instance, the rules of PIL often refer to connecting factors or perhaps a certain place, e.g. the place where the harmful event occurs (or may occur),⁴⁰ in order to determine either jurisdiction or applicable law. While conflicts lawyers may find these connecting factors and acts of localisation relatively easy to apply in a material or physical world, their application to the non-material world may prove a lot more difficult. The aim of this doctoral thesis is to shed as much light as possible on the perilous confluence. Another strained interface is that between PIL and Intellectual Property (IP) Law. Perhaps this is a consequence of the fact that PIL, in the strict sense of that term, has been slow in developing in the field of IP. As a result, both conflicts lawyers and IP lawyers have looked upon the interface between their respective fields as a disputed and dangerous, legal borderland.⁴¹ Over the past decade, a number of books analysing this complex interface have been written by the likes of Fawcett & Torremans, Drexl & Kur (eds), and Basedow (ed).⁴²

The advent of the ‘Information Society’ has awoken a fresh interest in choice of law for copyright and related rights, due to the fact that the production and use of information and information technologies have become of primary economic significance and the fact that modern communication technology offers new possibilities for massive and instantaneous distribution of information across geographic boundaries. By common admission, the arrival of the networked environment lays bare the shortcomings of the traditional territorial approach to copyright and related rights.

³⁹ However, the author concedes that not all internet communications traverse sovereign borders. It is fair to say, though, that a significant proportion of all internet communications are transborder in character.

⁴⁰ Brussels I Regulation, Article 5(3).

⁴¹ Stig Stromholm, ‘Preface’ in Jürgen Basedow et al (eds), *Intellectual Property in the Conflict of Laws* (Mohr Siebeck 2005) v.

⁴² See Annex 1 of this thesis where I have included a literature review of the principal works consulted during the writing of this thesis.

It has been argued that one of the reasons for the slow development of PIL in the field of IP is due to the fact that in most European countries, IP came into existence through successive developments of systems of individual *ad hoc* privileges strictly limited to the territory of the State granting them.⁴³ These historical roots were carried over with unfortunate consequences into the modern era. The challenge of trying to solve conflicts problems led to a *sui generis* solution at the end of the nineteenth century in the guise of international conventions, which do not even lay down rules for the choice of the applicable law.

1.6 The Interface Between the internet and PIL – Gradually Gaining in Prominence

Over the last few years, the theme of the internet/PIL interface has gradually begun to feature as a distinct theme in the legal literature. While Svantesson's *Private International Law and the Internet*, first published in 2007 (and now into its second edition, published 2012) is the most obvious example, it was not the pioneering monograph. That accolade belongs to the jointly edited work by Boele-Woelki and Kessedjian titled *Internet: Which Court Decides? Which Law Applies?*,⁴⁴ which dates from August 1998.

Two years prior to the appearance of Svantesson's second edition, Wang published her work *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China*.⁴⁵ This text has, as its core, electronic commerce transactions, not IP infringements. Online dispute resolution, B2B contracts and B2C contracts in the EU, US and China constitute the various elements of this work.

Fawcett and Torremans' *Intellectual Property and Private International Law* also explores the internet/PIL intersection but *only* within the context of the primary theme of the IP/PIL interface.

⁴³ Stig Stromholm, 'Preface' in Jürgen Basedow et al (eds), *Intellectual Property in the Conflict of Laws* (Mohr Siebeck 2005) v.

⁴⁴ Katharina Boele-Woelki and Catherine Kessedjian (eds), *Internet: Which Court Decides?, Which Law Applies? Quel tribunal decide? Quel droit s'applique?* (1st edn, Kluwer Law International 1998) 23.

⁴⁵ Faye Fangfei Wang, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (1st edn, Cambridge University Press 2010).

Somewhat surprisingly, in contrast with the legal literature, PIL legislation adopted at EU level over the last thirteen years or so (i.e. Brussels I, Rome I and Rome II) only makes scant reference to the internet and then, only in an oblique way.⁴⁶ It is regrettable that the internet did not loom large in the EU legislators' collective consciousness when they were drafting the three regulations just mentioned.⁴⁷

Despite the fact that PIL has been intensively studied by continental jurists since the 13th century and that the first rules of English conflict of laws can be traced back to the late 17th century,⁴⁸ tensions arise when this field of law, dependent on sovereign borders for the efficacy of its application, confronts the amorphous 'territory' of the internet.

⁴⁶ The tangential reference to the internet is made in Recital (24) of Rome I when reference is made to a Joint Declaration by the Council and the Commission on Article 15 of the Brussels I Regulation. Article 15 relates to Jurisdiction over Consumer Contracts and the targeting by an undertaking of its commercial activities at a Member State of the consumer's residence. In their joint declaration, the Council and Commission state that 'the mere fact that an internet site is accessible is not sufficient for Article 15 to be applicable, although a factor will be that this internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance.' Interestingly, the E-Commerce Directive (Directive 2000/31/EC) does make reference to private international law at Recital (23) and Article 1(4). Recital (23) confirms that the E-Commerce Directive does not aim to establish additional PIL rules or deal with the jurisdiction of the courts. Somewhat oddly, it goes on to provide that applicable law provisions must not restrict the freedom to provide information society services as established in the E-Commerce Directive. The Directive on Enforcement of IPRs (Directive 2004/48/EC) has a similar provision to the E-Commerce Directive. Its Recital (11) provides that the Directive 'does not aim to establish harmonised rules for judicial co-operation, jurisdiction, the recognition and enforcement of decisions in civil and commercial matters, or deal with applicable law.' It acknowledges that there are Community instruments which govern such matters in general terms and are, in principle, equally applicable to intellectual property. The InfoSoc Directive (Directive 2001/29/EC) contains no reference to PIL.

⁴⁷ Of course, the adoption of the E-Commerce Directive in 2000 shows that the legal aspects of Information Society services were already in the minds of EU legislators at the start of the new millennium.

⁴⁸ Lord Collins of Mapesbury et al (eds), *Dicey, Collins and Morris: The Conflict of Laws*, vol 1 (15th edn, Sweet & Maxwell 2012) 9 et seq. In fact, conflict of laws first came to prominence in English courts towards the end of the 18th century, mainly because of conflicts

This may be due to the relatively recent emergence of the internet as a common medium of communication and dissemination, or perhaps, the fact that PIL has undergone significant changes in the past decade. This is particularly evident at EU level where three major PIL regulations, relevant to this thesis, have been adopted since 2000.⁴⁹ Brussels I (jurisdiction) was adopted in 2001 while the two applicable law regulations; Rome I (contractual obligations) and Rome II (non-contractual obligations) were adopted in 2008 and 2007 respectively. At Hague Convention level too, the long-awaited Convention on Choice of Court Agreements⁵⁰ was only concluded in June 2005. In essence, therefore, the world of conflicts law is still in a relative state of flux and quite possibly conflicts experts prefer to observe evolutions (legislative and jurisprudential) and wait for the legal landscape to take on a more definite shape before proffering opinions on how the adapted (or new) conflicts frameworks might be applied to the online world. Perhaps the recent interest in ‘national solutions’ such as the French HADOPI⁵¹ and the UK’s Digital Economy Act 2010,⁵² as well as contractual models such as the Graduated Response approach reflect the unsatisfactory nature of a rule-based approach?

This thesis deals with a novel subject matter, but, given the newness of the subject matter, the author readily acknowledges that more than one interpretation of the central issue of this thesis exists. As a type of corollary, conflicts experts will undoubtedly differ as to the ease or difficulty of applying PIL rules/provisions to the internet. The reality is that disagreements are inevitable. We are still at a very early stage in the

between the laws of England and Scotland. In the 19th century, its development was enormously accelerated by the rapid increase in commercial and social intercourse between England and Continental Europe and with the British territories overseas.

⁴⁹ Prior to the adoption of the Brussels I Regulation and the Rome 1 Regulation, there existed two predecessor conventions: the 1968 Brussels Convention on Jurisdiction and Enforcement in Civil and Commercial Matters and, the 1980 Rome Convention on the Law Applicable to Contractual Obligations.

⁵⁰ This convention is what remains of previous plans of the Hague Conference to formulate a convention on jurisdiction and recognition/enforcement of foreign judgments. The plans were scaled back significantly in late 2003. The narrower scope of the new convention means that it will only apply to parties in a contractual situation and therefore will not cover instances of online tortious copyright infringement.

⁵¹ See para 7.3.4.

⁵² See para 7.3.3.

application of PIL rules/provisions to an online environment, and, in many ways, there are no definitive answers to the issues raised in this thesis. Part of my task is to pinpoint the actual tort PIL rules that prove challenging to apply in an online environment and to determine whether technology, legislation or judge-made relief (or a combination of all three) can be used to ameliorate the situation.

1.7 Originality of this Work

Chapter 6 accounts for a considerable proportion of the originality in this thesis. In that chapter, online copyright infringement and online defamation are critically evaluated to determine how compelling the analogue of online defamation is. Much of this evaluation is carried out in the context of localisation, and points of connection and disconnection are identified as between the two torts. The media used to commit the infringements are analysed from the viewpoint of ‘push’ or ‘pull’ technology.

This thesis’ originality is also strongly linked to the confluence at which it is located. It is, in effect, located at the point where three distinct fields of law meet: PIL, IP Law and Information Technology Law. Considerable tensions exist between the field of PIL and IP. Similar (and more easily understandable) differences exist between territory and sovereign borders-oriented PIL and the de-territorialised internet.

Much of the novelty of this thesis derives from the fact that it starts from the premise that the interface between PIL and the internet will *not* be an entirely smooth one. In this thesis, there is an implicit acknowledgement that the PIL rules/laws alone may not be enough. For a provision like Article 2, Brussels I, to work effectively, there may well have to be reliance on some or all of the following elements: geolocation technology, equitable relief (*Norwich Pharmacal* orders/blocking injunctions) and data retention legislation. In sum, this means that the black letter law alone may be inadequate (or, insufficient) and that its efficacy will possibly depend on a ‘coalition’ of technology, equitable relief and IT law.

By analysing the PIL/IP intersection from a decidedly technological perspective, I do something that was not done by Fawcett and Torremans in their work *Intellectual*

Property and Private International Law.⁵³ While Fawcett and Torremans' work draws attention to the distinct set of PIL challenges that arise with online IP infringements, their work does not explore the practical issues of proof as does this thesis. Their book does not seek to explore how PIL conundra in an online scenario can be resolved by searching *outside* PIL itself. My thesis, in contrast, explores how geolocation technology is gradually re-establishing physical borders on the internet, thereby assisting judges and conflicts lawyers alike.

By focusing on copyright, my thesis remains distinct from Svantesson's *Private International Law and the Internet* which focuses on online contracts and online defamation. Svantesson's work also covers trade marks, albeit rather superficially. While Svantesson treats geolocation technology in depth, he does not treat either equitable relief or data retention legislation, two elements which feature prominently in my PhD.

By attempting to deal with practical problems in a practical way, my thesis is distinguished from the more theoretical work of Fawcett and Torremans. By focusing exclusively on online copyright infringements, my thesis is distinguished from Svantesson's work which has a strong defamation/contracts focus and some *non-core* treatment of trade marks.

In short, my thesis addresses a gap in the legal literature and proposes solutions in situations when classic PIL rules are less than effective due to the presence of an online component.

1.8 Methodology: A Library-Based Research Study

I chose a functionalist comparative methodology as my thesis has a strong interdisciplinary character. My thesis is situated within a larger framework of other disciplines, most evidently Information and Communications Technology (with special focus on the internet). My doctoral research covers a gamut of technological issues, some of which are intrinsic to my overall conclusions. These include: geolocation technology, digital rights management, the BitTorrent protocol, data packets traffic on

⁵³ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011).

the internet and copyright infringements perpetrated by satellite or cable. Technological processes such as upload and download feature conspicuously too in the context of localisation.

While there is always a risk element in a comparative lawyer using disciplines foreign to his own, there is also the boon of better understanding one's own discipline by viewing it through the prism of foreign disciplines.⁵⁴

Of the seven functions⁵⁵ which comprise the functional method of comparative law, my thesis is built on three of them, namely, 1) the critical function of providing tools for the critique of law; 2) the evaluative function of determining the better law; and 3) the universalizing function of preparing legal unification.

Focusing on the universalizing function above, part of the functional method is to act as a tool for the unification of law. One of the traits of functionalism is to identify similarities among different laws, thereby enabling legislators to draft an optimal uniform law that overcomes and transcends the doctrinal peculiarities of local legal systems.⁵⁶ The draft International Copyright Code⁵⁷ devised by JAL Sterling in 2001

⁵⁴ According to Michaels, an interdisciplinary analysis yields 'three promises', namely (1) It should enable a (re-) construction of a more theoretically grounded functional method of comparative law than is usually presented. (2) It should help formulate and evaluate the concept in order to determine how functional the method really is. Just as comparative law can borrow from the development of functional methods in the social sciences, so it can borrow from the development of critique. (3) The comparison with functionalism in other disciplines may reveal what is special about functionalism in comparative law, and why what in other disciplines would rightly be regarded as methodological shortcomings may in fact be fruitful for comparative law. Ralf Michaels, 'The Functional Method of Comparative Law' (SSRN, 3 November 2005) 3

<http://papers.ssrn.com/so13/papers.cfm?abstract_id=839826> accessed 17 July 2012.

⁵⁵ Namely, 1) the epistemological function of understanding legal rules and institutions; 2) the comparative function of achieving comparability; 3) the presumptive function of emphasizing similarity; 4) the formalizing function of system building; 5) the evaluative function of determining the better law; 6) the universalizing function of preparing legal unification; and 7) the critical function of providing tools for the critique of the law. Ibid 19.

⁵⁶ Ibid 31.

⁵⁷ JAL Sterling, 'Draft International Copyright Code' (May 2001)

and the gradual establishment of a *de facto* international copyright code,⁵⁸ as described by Ginsburg in 2000 are both in this mould. Arguably, too, it is only once the functional similarities of different laws are realised, that it becomes easier to unify them on the basis of those similarities.

Highlighting as it does, the real and practical difficulties encountered by private international lawyers in the application of a certain set of PIL rules to the internet, it can be said of this thesis that its nature is both investigative and interpretative.

An example of comparative methodology in this thesis occurs in chapter 3 on transnational IP infringements. In that chapter, I purposely choose recent UK and CJEU court rulings to demonstrate firstly, the subject-matter diversity involved in online IPR infringement and, secondly, the geographic diversity apparent in such cases. Comparative methodology also features prominently in chapter 5 on the applicable law, particularly in my analysis on the relative advantages and disadvantages of adopting either a country of origin approach or a country of reception approach in the context of the applicable law.

While I certainly wore a comparatist's hat during the writing of this thesis, I also maintained a strong interest in trying to answer practical questions about the application of PIL in an online environment.

Besides the obvious comparative element in this work, I also deployed a fair degree of analogy. Sometimes, the source material was quite relevant though somewhat tangential to the core issue of this thesis. A good example of this is the Australian ruling in *Dow Jones & Company Inc v Gutnick*, analysed in depth in chapter .⁵⁹ Clearly, this judgment did not involve issues of digital copyright infringement but it did concern an online tort (defamation) and the elements of upload and download which, in turn, drew in issues of jurisdiction and choice of law. In chapter 6, I critically evaluate Svantesson's

<http://www.qmipri.org/documents/icc_english.pdf> accessed 13th August 2012.

⁵⁸ Ginsburg argued that national norms were being displaced and gradually superseded by a *de facto* international copyright code elaborated in multilateral instruments such as the Berne Convention, the TRIPs Accord and the then pending WIPO Copyright Treaty. Jane C Ginsburg, 'International Copyright: From a "Bundle" of National Copyright Laws to a Supranational Code?' (2000) 47 J Copyright Soc'y USA 265, 266.

⁵⁹ *Dow Jones & Company Inc v Gutnick* [2002] HCA 56.

defamation model to determine whether it is a useful framework for the analysis of copyright infringement.

1.9 Structure of Thesis

This thesis is divided into 10 chapters. The first chapter is a general introduction to the central theme of the doctorate. Chapter two describes the nature of the internet generally and also looks at the internet from the perspective of digital copyright. Trans-border IP infringement (principally copyright) forms the core of chapter three. In this chapter, I draw on a number of judgments from the UK and EU to demonstrate how multi-state IP infringement is becoming more commonplace. Chapters 4 and 5 are closely related as they look at the two key constituents of PIL, - jurisdiction and, the applicable law, respectively. Chapter 4 contains an indepth analysis of the case law arising from Article 5 (3), Brussels I and the Brussels Convention, 1968. Almost inevitably, Chapter 5 treats the applicable law and does so through a critical evaluation of legal instruments (the Rome II Regulation and the Berne Convention) and individual choice of law rules (e.g. the country of origin rule and the country of reception rule). Chapter 6 focuses on online copyright infringement and its analogue, online defamation. The main objective of this chapter is to identify the rules for localising the various torts online and the analysis is somewhat nuanced as the author looks at three of copyright's restricted rights. An intermeshing analysis occurs at chapters 7 to 9 inclusive. All three chapters focus on jurisdictional issues with chapter 7 dedicated to an examination of elements facilitative of the operation of Article 2, Brussels I, while chapter 8 is dedicated to an examination of elements non-facilitative to the operation of Article 2, Brussels I. Chapter 9 is somewhat distinct from the two previous chapters in that it has as its focus the special jurisdiction provision - Article 5(3), Brussels I. Much of this chapter is given over to the analysis of the landmark ruling, *Dow Jones v Gutnick*⁶⁰ and how the High Court of Australia determined the *locus* of an online defamation. Chapter 10 contains my general conclusions and provides answers to the five research questions contained in this chapter.

1.10 Summing Up

This introductory chapter sets out many of the key elements of this thesis, to include its objectives, the rationale for choosing online copyright infringement as the primary

⁶⁰ Ibid.

research component, the scope of the thesis, my research questions, my original contribution to legal science, my methodology and my chapter structure.

Chapter 2: The Nature of the Internet

TABLE OF CONTENTS

The Internet	42
2.1 The Internet – A network of computers and servers	43
2.2 An Open, cooperative, flexible and decentralised medium	44
2.3 Tensions between the internet and copyright	45
2.4 Border-disregarding	47
2.5 The internet in China – a four-tier system	47
2.6 Geographical independence	48
2.7 Low-threshold information distribution	48
2.8 Portability	49
2.9 Nature of the Internet (as seen from the copyright perspective)	49
2.9.1 The seamlessness of the Internet	50
2.10 Characteristics of Infringement over the Internet	51
2.10.1 Problems of identity and location of the parties	51
2.10.2 Difficulty in locating where the act of infringement occurred	51
2.10.3 Ubiquitous and multi-state Infringement.....	54
2.10.5 How today’s digital content landscape has been impacted by P2P	55
2.10.6 Other facets of the Internet	58
2.11 The EU’s PIL framework and its protective scheme for consumers	58
2.12 The internet – bordered or borderless?	61
2.13 Conclusions	63

2.1 The Internet – A network of computers and servers

In essence, the internet is a network of computers and servers,⁶¹ a network that, by its very nature, crosses sovereign borders. Its transnational character virtually guarantees that issues of PIL will arise when disputes are litigated. The internet enables access to and communications of information. These bits of information are routed almost randomly to their destination in small packets that travel via different routes and are reassembled on arrival.⁶²

As the information is sent in digital format, there is hardly any limit to the kind of information that can be sent. Digitised data, text, graphics, music, pictures and films are capable of dissemination over the internet. All the aforementioned are, of course, subject-matter in which copyright may subsist. The internet facilitates the exploitation, use and infringement of IPRs on a cross-border and regular basis⁶³ with peer-to-peer systems such as Gnutella, eDonkey, FastTrack, and Bit-Torrent being good examples of entities which facilitate IP infringement.⁶⁴ A combination of significant advances in personal computing power, increased power of internet connectivity, the emergence of portable devices such as smart phones and tablets, increased internet speeds and high quality reproductions together create the perfect technological environment for those

⁶¹ Julia Hörnle, 'The Jurisdictional Challenge of the Internet' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009) 121.

⁶² Andrew Murray, *Information Technology Law – The Law and Society* (2nd edn, Oxford University Press 2013) 21.

⁶³ See James Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 535.

⁶⁴ For a good account of the impact of P2P piracy on today's digital content landscape, see Wan Man Jason Fung and Avnita Lakhani, 'Combating peer-to-peer file sharing of copyrighted material via anti-piracy laws: issues, trends and solutions' (2013) 29 *Computer Law & Security Review* 382-402. The following works also treat peer-to-peer in comprehensive form: Alain Strowel (ed), *Peer-to-peer file sharing and secondary liability in copyright law* (Edward Elgar 2009); Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law* (4th edn, Routledge 2012) 333-348; Andrew Murray, *Information Technology Law – The Law and Society* (2nd edn, OUP 2013) 263-291; and Paul Torremans, *Holyoak and Torremans Intellectual Property Law* (7th edn, OUP 2013) 654 et seqq.

intent on illegally reproducing and disseminating protected material.⁶⁵ The proliferation of illegal peer-to-peer activity is testament to the use of the internet for unlawful activities.

2.1 An Open, cooperative, flexible and decentralised medium

Since its inception as a commercial medium in the mid-1990s the internet has evolved into an open,⁶⁶ cooperative, flexible and decentralised⁶⁷ medium. Over the past twenty years, it has become a communication and distribution medium *par excellence*.

It is also presented by stakeholders as a tool for entrepreneurship and commerce. In terms of entrepreneurship, e-commerce is particularly strong in the UK. Of all the G20 countries, it is to the UK economy that the internet contributes the greatest share of GDP.⁶⁸ E-tailers such as Marks & Spencer and John Lewis ensure that the UK retains a particularly strong position within the OECD in terms of the proportion of its nationals who order/purchase goods or services online (64% in 2011).⁶⁹ As regards commerce, the internet is now the default platform for legal music subscription services such as Spotify, Deezer, Napster Unlimited and eMusic.

⁶⁵ Wan Man Jason Fung and Avnita Lakhani, 'Combatting peer-to-peer file sharing of copyrighted material via anti-piracy laws: issues, trends, and solutions' (2013) 29 *Computer Law & Security Review* 382, 383 et seq.

⁶⁶ Bellia, Schiff Berman and Post interpret the term 'open' as meaning easy to join, with no central server that must be informed of a new network participant, in order to communicate with others over the internet one need only obtain the necessary software and arrange for a connection to any one of the thousands of ISPs worldwide. Patricia Bellia, Paul Schiff Berman and David Post, *Cyberlaw, Problems of Policy and Jurisprudence in the Information Age* (3rd edn, Thomson West 2007) 16.

⁶⁷ In *Dow Jones v Gutnick* [2002] HCA 56 [80], Kirby J in the Australian High Court described the internet as a 'decentralised, self-maintained telecommunications network'. See also Joanna Kulesza, *International Internet Law* (1st edn, Routledge 2012) 142.

⁶⁸ Hannah Kuchler, 'UK "leads the world" in e-commerce' (*Financial Times*, 19 March 2012) <<http://www.ft.com/cms/s/0/ef3e1a04-71b4-11e1-8497-00144feab49a.html#axzz2yDydFfej>> accessed 7 April 2014.

⁶⁹ HM Government, European E-Commerce Taskforce, 'Empowered Consumers, Unleashed Business' (August 2013) 5 <<http://dpalliance.org.uk/wp-content/uploads/2013/09/EU-e-commerce-taskforce-FINAL-REPORT.pdf>> accessed 7 April 2014.

2.2 Tensions between the internet and copyright

The coming of each new technology has meant re-thinking and re-balancing copyright law.⁷⁰ In fairly rapid succession, innovations such as the photocopier, the audio cassette deck, the VCR, DVDs, CDs and CD-Roms have all challenged that law and with the introduction of each new technology, it is tested and evolves accordingly.⁷¹ At a more sophisticated level of information distribution, satellite broadcasting,⁷² streaming⁷³ and cable (re-) transmission have also posed serious challenges to copyright, particularly so given the fact that they frequently possess a transnational character.

Copyright and copyright material have been particularly imperilled since the emergence of the internet as a commercial medium in the mid-1990s. Indeed, the internet could, with justification, be described as the greatest copying machine ever invented as copying of protected works occurs constantly and necessarily.⁷⁴ Cornish, Llewelyn and Aplin go further and describe the relationship between the internet and copyright as ‘the most inflamed issue in current intellectual property.’⁷⁵ They point to the extraordinary ease and accuracy with which the internet distributes literary, artistic, musical and audio

⁷⁰ For instance, see Isabella Alexander, ‘All change for the digital economy: some observations from the history of copyright’ (2010) 28 Copyright Reporter: Journal of the Copyright Society of Australia 215-228.

⁷¹ Diane Rowland, Uta Kohl and Andrew Charlesworth, *Information Technology Law* (4th edn, Routledge 2012) 334.

⁷² See, for instance, the example given by Paul Goldstein and P Bernt Hugenholtz in their work *International Copyright: Principles, Law and Practice* (3rd edn, OUP 2013) 127 (unauthorised transmission of a musical work by satellite to another country).

⁷³ See Case C-607/11 *ITV Broadcasting Ltd v TVCatchup Ltd* [2013] 3 CMLR 1, in which the CJEU held that unauthorised streaming of free-to-air television broadcasts to persons within the catchment area does amount to a new transmission to the public within Article 3 of the InfoSoc Directive if it is performed by an organisation other than the original broadcasting organisation, since it involves the distribution of the broadcast by a different technical means from that used for the distribution of the original broadcast. See Mark Hyland, ‘TV Broadcasters’ IP rights bolstered by recent CJEU preliminary ruling’ (2013) *Law Society Gazette* 58, 59.

⁷⁴ Two common examples include: where a software program is loaded into a computer RAM, or a surfer opens up a webpage.

⁷⁵ William Cornish, David Llewelyn and Tanya Aplin, *Intellectual Property: Patents, Copyright, Trademarks and Allied Rights* (8th edn, Sweet & Maxwell 2013) 858.

visual material held in digital format.⁷⁶ Material accessed on websites, chatrooms, email services and social networking sites can be transmitted over and over again without loss of quality.⁷⁷

The reality of the internet is that electronic copying, whether ephemeral or more permanent in character, occurs all along the internet chain, from point of upload to point of destination. Given the ease of unauthorised dissemination of copyright material across sovereign borders, cross-border litigation becomes inevitable and, as a consequence, PIL issues arise.

YouTube is a good example of an internet platform upon which copyright laws are frequently, though perhaps inadvertently, flouted, while defamatory comments are tweeted or posted from/to social media with ever increasing frequency.⁷⁸ In chapter 6, I shall critically evaluate the points of connection and disconnection which exist between online copyright infringement and online defamation.

As to the cooperative nature of the internet, its manifestation can be seen in blogs, threads, discussion groups and legal peer-to-peer activities. But, the flipside of legal cooperation is illegal cooperation, and this is most obvious in peer-to-peer activity involving unauthorised file-sharing (both music and movies).

⁷⁶ Ibid.

⁷⁷ Ibid.

⁷⁸ As regards Twitter, see the High Court ruling, *The Lord McAlpine of West Green v Sally Bercow* [2013] EWHC 1342 (QB); As regards Facebook, the High Court in Northern Ireland stated on 6th February 2013 that £35,000 should be awarded against an unknown person who libelled two company directors and a staff member on Facebook. BBC, 'Judge rules three were defamed on Facebook' (*BBC News Northern Ireland*, 6 February 2013) <<http://www.bbc.co.uk/news/uk-northern-ireland-21354945>> accessed 8 April 2014. There is also the Irish High Court ruling handed down by Mr Justice Peart on 16th May 2013, - *Eoin McKeogh v John Doe and Others* (Record No. 2012/254P) - in which an interlocutory injunction was granted against Facebook and Google requiring them, YouTube, and a number of websites to permanently remove a video and accompanying material which wrongly identified a man dodging a taxi fare and defamed him with a series of offensive comments.

2.3 **Border-disregarding**

As a medium of communication, the internet works largely independently of geographical borders.⁷⁹ In this regard, it is very similar to telephone communication, and can be contrasted with postal mail which is still dependent on such borders (parcels can be intercepted/opened by customs officers at national borders to ensure compliance with national quarantine requirements).⁸⁰

In general, internet communications can flow freely between most countries without there being any border checks. However, certain countries such as China, Saudi Arabia and Iran choose to exercise a degree of border control which often involves blocking access to material held on foreign servers.⁸¹

2.4 **The internet in China – a four-tier system**⁸²

The bottom tier (i.e. fourth tier) comprises individual internet users. They connect to the internet through the Internet Service Providers (ISPs) (tier three). The ISPs connect to an Internet Access Provider (IAP) (second tier). In fact, it is the IAPs who actually own the physical networks, which are then leased by the ISPs. Finally, the IAPs connect to the government's gateway (first tier) and can thereby access the global internet. What

⁷⁹ Taubman describes the internet as being 'famously blind to national boundaries'. Antony Taubman, 'International Governance and the Internet' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009) 18

⁸⁰ Dan JB Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 34.

⁸¹ See Nikolaos Koumartzis and Andreas Veglis, 'Internet regulation: The need for more transparent internet filtering systems and improved measurement of public opinion on internet filtering' (2011) 16 *First Monday* <<http://firstmonday.org/ojs/index.php/fm/article/view/3266/3071>> accessed 8 April 2014. Also see Murray's account of State filtering/content blocking. He refers to the Open Net Initiative which lists substantial filtering in fifteen different countries along with strong suspicions that Cuba and North Korea also deploy extensive filtering practices. Andrew Murray, *Information Technology Law - The Law and Society* (2nd edn, OUP 2013) 75 et seq.

⁸² Dan JB Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 34 et seq.

makes this system distinct is the fact that it is the system prescribed by law.⁸³ As a consequence, internet users in China are not permitted to connect to the internet via a foreign ISP in order to circumvent the system. A similar structure can be found in Saudi Arabia. In contrast, most other countries do not exercise any effective border control and internet communications, both domestic and foreign, go through a multitude of private and public carriers. This ensures the absence of strangle points. Svantesson then draws a distinction between the ‘international internet’ which he describes as borderless and the domestic sub-internet in China which he describes as borderless only within China but not in relation to the rest of the world.⁸⁴

2.5 Geographical independence

Internet communication is available to people regardless of their geographical location. For individuals seeking information, the geographical location of that information is virtually irrelevant in most forms of internet communication.⁸⁵ Clicking on a hyperlink provides access to the relevant information even if it is stored on a server many thousands of miles away. Stated differently, someone using the internet can move effortlessly over great geographical distances and between different states.⁸⁶ Another aspect of internet communication is its instantaneousness. There is no great time difference between accessing a website hosted on a local server and accessing a website hosted on a server located on the other side of the world.⁸⁷

2.6 Low-threshold information distribution

In general, ordinary individuals do not have the technical knowledge or the financial ability to use forms of communications such as television and radio broadcasts; these forms are ‘reserved’ for more sophisticated operators such as media organisations.

⁸³ Ibid 35, where he refers to the Interim Rules of the People’s Republic of China on International Interconnectedness of Computer-based Information Networks (promulgated on 25 April 2007).

⁸⁴ Ibid.

⁸⁵ In the Digital Age, there is no guarantee that digital content will actually be stored in the country where its owner resides. This is particularly true in the case of companies which may store content on web servers abroad. For instance, see the facts of *Dow Jones & Company v Gutnick* [2002] HCA 56.

⁸⁶ Dan JB Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 36.

⁸⁷ Ibid.

However, ordinary individuals can, with relative ease, impart all kinds of information via the internet, through social networking or e-mail. Needless to say, sometimes the material being disseminated online infringes copyright.

Technical limitations in the form of uploading limits can be imposed by ISPs so that internet users are frequently connected to the internet under arrangements that provide much greater downloading allowance than uploading allowance. This hampers and restricts the user's ability to disseminate information.⁸⁸ Subject to this, another important aspect of online information distribution is that of re-dissemination. Once an individual comes into possession of a copyright work, he can relatively easily re-disseminate that work without any loss of quality.

2.7 Portability

Portability is a key characteristic of the internet; a very simple example of such being the e-mail. An e-mail can be sent from an internet-connected device anywhere in the world. Mirror websites can be accessed via two or more servers anywhere in the world. A particular website might have its text located on a server in New Zealand while the photographs are stored on a server in Brazil.⁸⁹ Naturally, the vast majority of internet users will not even be aware of this 'bifurcation'.

Sometimes the websites are spread between two or more servers so as to ensure a faster service for those accessing the service or so as to avoid congestion. Caching servers are often used to 'deliver' a web page's 'heavy' items, e.g. pictures and video clips. In such cases, the original web server will be 'bypassed' and the nearest available cache will instead be requested.⁹⁰ Portability causes considerable problems in relation to PIL, particularly as regards localisation.

2.8 Nature of the Internet (as seen from the copyright perspective)

The internet has established a new form of worldwide communication which guarantees international supply and exchange of information in electronic form. Websites are the

⁸⁸ Ibid 39.

⁸⁹ Ibid 42.

⁹⁰ Akamai's caching services is referred to in 'Geography and the Net - Putting it in its place' *The Economist* (9 August 2001); Dan JB Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 42.

repositories of huge quantities of material thanks to sophisticated methods of digital storage. A work put on the internet can be accessed by individuals in all parts of the world and can then be copied and further disseminated.⁹¹

But this widescale access to works which have been placed on the internet throws into question the concept of publication (putting copies at the disposal of the public) in the copyright community. This is linked to the ‘making available’ right (cross reference). The economic rights of communication to the public and ‘making available’ to the public⁹² can become quite blurred in an internet context when an unpublished work is posted on the internet and then can be accessed simultaneously in many different countries.⁹³

2.8.1. The seamlessness of the Internet

By ignoring national boundaries and operating, by definition, on a cross-border basis, the internet’s seamlessness ensures that netizens unconsciously cross state boundaries while websites are often as accessible to those living abroad as they are to those living in the state which hosts the website.⁹⁴ However, despite the unquestioned trans-border nature of the internet, there are always territorial connections with various states.⁹⁵ For example, both the claimant and the defendant in copyright litigation will be resident/domiciled in a particular state, and both the uploading of information (infringing material) and the downloading of that information will, of necessity, occur in specific States.

⁹¹ JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 33.

⁹² Both these rights are examined in detail in chapter 6.

⁹³ *Ibid.*

⁹⁴ The seamlessness of the internet can be viewed from two perspectives - that of the netizen (who moves seamlessly between zones governed by differing regulatory regimes in accordance with their personal preferences), and that of internet content, which flows seamlessly over physical borders. See: Andrew Murray, *Information Technology Law - The Law and Society* (2nd edn, OUP 2013) 49. The seamlessness of the internet is ‘interrupted’ by the world’s more authoritarian regimes where filtering and blocking is implemented for a variety of reasons. This issue will be analysed later in this chapter.

⁹⁵ See, generally, Chris Reed, *Internet Law: Text and Materials* (2nd edn, CUP 2004) 7.1.2.

2.9 Characteristics of Infringement over the Internet

2.9.1. *Problems of identity and location of the parties*

A claimant who has been the victim of an online IP infringement may not know the identity of the defendant or where he is resident. Electronic addresses do not necessarily signify a geographical connection. For example, the tortfeasor may have an electronic address with a service provider whose domain name comprises a national identifier, such as 'UK', but that does not mean that he is resident in the UK.

2.9.2 *Difficulty in locating where the act of infringement occurred*

Frequently, when determining issues of jurisdiction, courts will have to identify the place where something has happened or threatens to happen. For example, a court may have to pinpoint the place where the tortious act giving rise to damage occurred or the place where the tort was committed. This task is problematic enough in non-internet cases but the difficulty is exacerbated with online copyright infringement.⁹⁶ Since communication over the internet involves a whole sequence of events between the original uploading of infringing material and its eventual downloading abroad, it can be difficult to localise the precise point where the actual infringement has happened.⁹⁷

Sterling describes the sequence of events as comprising the following: uploading of information; digitisation of the work; storage of the digitised form of the work; conversion of the digitised form of the work into the carrying signal; transmission of the carrying signal; reception of the carrying signal in the receiving machine; downloading

⁹⁶ James Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 538.

⁹⁷ *Ibid.* Interestingly, as far back as 1964, FA Mann recognised the problems associated with localisation in the context of modern communications technology and cross-border media. While his reference was aimed at things like telephone, teleprinter, television and international advertising, he pointed out that the distribution of content across a multitude of countries might mean that territorial connecting factors were too readily satisfied, and would generate dissatisfaction with the rigidity of present rules. Arguably, these deficiencies and dissatisfaction have multiplied with the ever increasing use of the internet for cross-border transactions and interactions. Frederick A Mann, 'The Doctrine of Jurisdiction in International Law' (1964) 111 *Recueil des Cours*, 1-162.

(storage of information in the memory of the machine); screen display, and, possibly, print out of display material. This sequence may involve numerous countries and, in the more complex cases, the transmission may travel via intermediate computers located in countries outside the originating and destination countries. One could argue that an online act of infringement is truly multi-national in character.⁹⁸

The problem of locating the infringing event can be compounded when the substantive law of infringement does not specify sufficiently clearly what the act of infringement is, or fails to define certain of its key concepts for an online environment.⁹⁹ Initially, copyright infringements were conceived to occur entirely in one particular country (a single act leading to a single effect), but the internet has uprooted that concept entirely. However, despite the complex sequence of events, there are still only two really significant occurrences in the whole chain – those of uploading and downloading. Together, they constitute the two constants that will be apparent if the matter proceeds to litigation.¹⁰⁰ Between uploading and downloading, the route that the information

⁹⁸ JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 144, 150 et seqq, 652 et seq, and 659 et seq.

⁹⁹ James Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 542. Two key economic rights under copyright law are those of reproduction and communication to the public. But, where will the reproduction take place if one sends a request to a server for protected content which is then sent to the requestor and displayed on his screen. The requestor's screen will undoubtedly be a place of where reproduction occurs but there may be other reproductions along the way in intermediate countries. Likewise, is placing material on a website so that others can access it when they wish, an act of communication to the public?

¹⁰⁰ In contrast, in terms of online defamation, following *Dow Jones v Gutnick* [2002] HCA 56, the place of download really is the preeminent locus. In the principal judgment in that case, it was made clear that damage to reputation can only occur when the defamatory material is in comprehensible form. And that only occurs when it is downloaded to the computer of the person who has pulled the material from a web browser (the publishee) (see para [44] of the judgment). See chapter 9 for a comprehensive treatment of the *Dow Jones* ruling. There is also the interesting High Court ruling *Ashton Investments Ltd v OJSC Russian Aluminium (Rusal)* [2006] EWHC 2545 (Comm) which concerned allegations of computer hacking. Like the Australian High Court, the English High Court attached considerable importance to place of download. There, the relevant computer server was located in London but the hack originated from Russia. Hirst J (sitting as a Deputy Judge of the High Court) ruled that

(bits) takes can vary greatly from case to case, depending on whether a server is used in a third country. In a case where copyright material is downloaded abroad without permission from the rightsholder, which court should have jurisdiction over this cross-border activity? Should it be every state in which the downloading takes place? Conceivably, therefore, the courts of approximately 200 countries could assume jurisdiction (albeit they would be very unlikely to do so concurrently), each exercising jurisdiction over the specific act of copyright infringement occurring in its own territory. Arguably the act of uploading makes for a considerably easier localisation as the uploading often only takes place in one state.¹⁰¹ Matters can become complicated however where one uploads in country A but the infringing material is then placed on a server which hosts the relevant website in country B.

‘significant damage had occurred in England where the server was improperly accessed and the confidential and privileged information viewed and downloaded’ (at para [62]). *Ashton Investments Limited* was recently relied on by counsel for the claimants in *Judith Vidal-Hall and others v Google Inc* [2014] EWHC 13 (QB) [78], a case involving allegations of misuse of private information, breach of confidence and breach of the Data Protection Act 1998.

¹⁰¹ Article 1(2)(a) of Directive 93/83/EEC on Satellite Broadcasting and Cable Retransmission opts for a practical rule of upload as it localises all communications to the public by satellite in the Member State where the programme carrying signals are ‘introduced into an uninterrupted chain of communication leading to the satellite’. For a Scottish judgment that seems to adopt a place of upload rule in an online copyright context, see *Alan MacKie t/a 197 Aerial Photography v Nicola Askew, Largsholidaylets.co.uk* [2009] SLT (Sh Ct) 146. The ruling gives the pursuer the right to initiate proceedings in the court of the place where the damage occurred or in the court of the place where the event giving rise to the damage occurred (i.e. the place where the illegal uploading by the defender of the pursuer’s copyright photographs took place). In their analysis of the ruling, Fawcett and Torremans argue that the court arguably adopts a place of uploading rule as the presiding Sheriff stated that the critical question was the location of a wrong that was committed by way of the internet (see para [30] of the judgment). In their view, this could only refer to actions by the defendant and, therefore, the crucial action in this sequence of events was the act of upload. James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 561.

2.9.3. *Ubiquitous and multi-state Infringement*

Fawcett and Torremans argue that internet-related cases also inevitably show a high incidence of ubiquitous infringement or at least multi-state infringement.¹⁰² This assertion stands to reason particularly as the internet is a means of communication which ignores national boundaries and infringing material can be (and often is) disseminated with consummate ease.

A good example of multi-state infringement is the 2013 ruling of *EMI Records v British Sky Broadcasting*.¹⁰³ The case, a website-blocking application under Section 97A, CDPA 1988, concerned three websites. Mr Justice Arnold's ruling pointed towards a high degree of online trans-border copyright infringement. For instance, the operators of the copyright infringing websites appeared to be based outside the UK.¹⁰⁴ All three websites had significant numbers of visitors from the UK with KAT experiencing 3.7 million visitors in June 2012 alone.¹⁰⁵ The same website offered users a choice of between 28 different languages which facilitated and encouraged the widest possible participation in the use of its services by P2P file-sharers.¹⁰⁶ In addition, all three websites repeatedly shifted between various ISPs based in different countries. The most prolific – KAT – had moved between ISPs based in eight different countries.¹⁰⁷

Fawcett and Torremans assert that 'unregistered rights such as copyright exist globally' and that the illegal posting of a protected work on the internet constitutes an

¹⁰² James Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 549. See also Julia Hörnle, 'The Jurisdictional Challenge of the Internet' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009) 133, where the author states: 'Since the internet can be accessed from anywhere in the world, the harm caused by an information tort committed on the internet may, in some cases at least, fall anywhere and everywhere'.

¹⁰³ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch). Dealt with in detail at para 6.10.2, where the ruling is analysed in the context of localisation of the communication to the public right.

¹⁰⁴ *Ibid* [48].

¹⁰⁵ *Ibid* [16]–[19].

¹⁰⁶ *Ibid* [53].

¹⁰⁷ *Ibid* [63].

infringement ‘in every single country in the world’. In my view, their assertion that copyright exists globally is exaggerated as copyright subject-matter is just as territorial as patents or trademarks, even if there is no requirement for it to be registered. It is not for nothing that copyright-protected material is sometimes referred to as a ‘UK copyright’ or, a ‘German copyright’, depending on where the material was first created/fixated. The territorial nature of copyright is underscored by Article 3 of the Berne Convention where the link between copyright protection and Berne Union countries is made.

Nor do I agree with Fawcett and Torremans’ argument that an act of posting infringing material on a website without the permission of the copyright holder potentially constitutes an infringement ‘in every single country in the world’.¹⁰⁸ While there may be a slender case for contending that an online infringement may ‘spread’ geographically by virtue of Berne Union considerations, there is still some conceptual distance to travel before one could accept that the infringement occurs ‘in every single country of the world’.

Frankly, it is difficult to see how the posting of infringing material on one particular website involves an infringement in every country of the world. A mere accessing of the infringing material could arguably create a RAM copy in the accessor’s internet-enabled device, but the internet and easy internet access is built on an inevitable ‘system’ of implied licences. It is asserted that a primary infringement would be focused on one particular country but that conceivably (albeit improbably) a secondary infringer could disseminate the infringing material far and wide, potentially making the infringement more than just local in nature.

2.9.4. How today’s digital content landscape has been impacted by P2P

The existence and development of P2P file-sharing software has an increasingly significant impact on the evolving digital content economy. First used in 1999 under the

¹⁰⁸ James Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 549.

name Napster, P2P technology has more recently manifested itself by way of the following programmes: Gnutella, eDonkey, and and Bit Torrent.¹⁰⁹

Unlike Napster, which was based on a central server, the BitTorrent protocol operates in a decentralised manner. The small-sized ‘packets’ of data into which torrent files are broken are handled by both sources (seeders) and downloaders (peers or leechers).¹¹⁰

The net result of all this is that thousands of torrent files (each containing part of a protected work) are being shared without recognition of, payment to, or protection for the copyright owner.¹¹¹

And, as personal computer power increases and the use of portable devices – all of which can access P2P networks – intensifies, users can more easily process complex content of higher quality such as high-definition movies, music and live multimedia experiences.

Nowadays, technological development is such that the quality of reproductions rivals that of the original. A deadly combination of increased internet speeds and distribution software such as P2P enable users to share files of any size.¹¹² Using readily available consumer products, end-users can illegally copy original content and effortlessly distribute it far and wide with potentially disastrous consequences for the relevant rightholders.

¹⁰⁹ See Mark Taylor et al, ‘Digital Evidence from peer-to-peer networks’ (2011) 27 Computer Law & Security Review 647.

¹¹⁰ For a detailed account of how P2P services work (with particular focus on Bittorrent), see *Dramatico Entertainment Limited v British Sky Broadcasting Limited* [2012] EWHC 268 (Ch) [19].

¹¹¹ Wan Man Jason Fung and Avnita Lakhani, ‘Combatting peer-to-peer file sharing of copyrighted material via anti-piracy laws: issues, trends and solutions’ (2013) 29 Computer Law & Security Review 382, 383.

¹¹² Ursula Smartt, *Media and Entertainment Law* (1st edn, Routledge 2011) 346.

Clearly, the question of copyright law in the digital environment remains a pressing one.¹¹³ Despite the steady growth in licensed digital music services (such as iTunes, Spotify, Deezer (mainly France), JUKE and TDC (mainly Denmark)),¹¹⁴ there is still significant evidence of digital piracy and this is borne out by the statistics. According to IFPI's Digital Music Report (2013), the FBI estimated that business generated by Megaupload (before its closure by the FBI in February 2012) in terms of its unlicensed content file hosting was worth USD175 million while the estimated damage to the creative industries was in the region of USD500 million.¹¹⁵ Figures contained in MusicMetric's Digital Music Index Report for the first six months of 2012 point to 345 million tracks downloaded illegally via BitTorrent.¹¹⁶ Similarly negative figures appear in the International Chamber of Commerce-commissioned report 'Building a Digital Economy: The Importance of Saving Jobs in the EU's Creative Industries'. That report focused on the link between internet diffusion and the decrease in recorded music sales. It highlighted the 36% fall in physical recorded music sales during the period 2004-2008, representing financial losses of close to €4 billion in that five year period.¹¹⁷

¹¹³ Hector L MacQueen, "'Appropriate for the Digital Age'?" Copyright and the Internet: 1. Scope of Copyright' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009) 184.

¹¹⁴ It is interesting to note that subscription services are now the fastest growth area in digital music with subscriber numbers up 44% in 2012 and revenues up 59% in H2, 2012. Spotify's paying subscribers now number more than 5 million up from 3 million in 2011. IFPI, 'IFPI Digital Music Report 2013 – Engine of a digital World' 14 <<http://www.ifpi.org/content/library/DMR2013.pdf>> accessed 16 April 2014.

¹¹⁵ Ibid 31.

¹¹⁶ See BPI, 'Digital Music Nation' (2013) 24-29 <https://www.bpi.co.uk/assets/files/BPI_Digital_Music_Nation_2013.PDF> accessed 16 April 2014.

¹¹⁷ TERA Consultants, 'Building a Digital Economy: The Importance of Saving Jobs in the EU's Creative Industries' (*International Chamber of Commerce/BASCAP*, March 2010) 21 <<http://www.droit-technologie.org/upload/dossier/doc/219-1.pdf>> accessed 16 April 2014.

2.9.5. *Other facets of the Internet*

2.9.5.1. *E-commerce and some of its protagonists*

While the principal focus of this thesis is online torts, another key dimension of the internet is e-commerce. Since the emergence of e-commerce in 1991,¹¹⁸ a number of companies have become well established in this sector. They are, for instance, eBay (consumer to consumer), Amazon (the world's largest online retailer), Yahoo (its e-commerce components include Yahoo Shopping, Yahoo Autos, Yahoo Real Estate, and Yahoo Travel), and Alibaba (more specifically, Taobao Marketplace). A salient feature of 21st century e-commerce is online booking, frequently used by consumers to book such things as hotels, cinema, theatre/concert tickets, various modes of travel (air, train and ferry), and holidays (package holidays and cruises).

2.10. The EU's PIL framework and its protective scheme for consumers

The EU's PIL framework encompasses a protective scheme for consumers, based on the philosophy that a consumer is in a weaker position relative to a company in a contract. This explains why PIL takes a biased position in favour of the consumer.¹¹⁹ This protective scheme revolves around two key PIL provisions, namely Article 15(1)(c) of the Brussels I Regulation and Article 6(1) of the Rome I Regulation. Both apply when the business (or professional) has pursued its commercial activities in the consumer's habitual residence or directs such activities to that country.

Article 15(1)(c), Brussels I refers to the business/entity which 'pursues commercial or professional activities in the Member State of the consumer's domicile or, by any means, *directs* such activities to that Member State or to several Member States including that Member State, and the contract falls within the scope of such activities.'

¹¹⁸ The start of e-commerce coincided with the National Science Foundation's decision to lift its ban on commercial businesses operating over the internet, thereby paving the way for Web-based e-commerce.

¹¹⁹ See for example Joined cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG; Hotel Alpenhof GesmbH v Oliver Heller* [2010] ECR I-12527, para 58, where the ECJ states as follows: 'As regards the latter provision (Article 15(1)(c), Brussels I), the Court has indeed repeatedly held that the special rules introduced by the provisions of the Brussels Convention on jurisdiction over consumer contracts serve to ensure adequate protection for the consumer, as the party deemed to be economically weaker and less experienced in legal matters than the other commercial party to the contract'.

Article 6(1) Rome I refers to a contract concluded between a professional and a consumer as being governed by the law of the country where the consumer has his habitual residence, provided that the professional (a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or (b) by any means, directs such activities to that country or to several countries including that country, and the contract falls within the scope of such activities

The notion of directing one's activities to the Member State of the consumer's domicile¹²⁰ within the meaning of Article 15(1)(c) of Brussels I was considered in Joined Cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG; Hotel Alpenhof GesmbH v Oliver Heller*.

Peter Pammer concerned a voyage contract (a consumer contract), which had been advertised in particularly attractive terms by a company whose seat was in Germany. The claimant, Peter Pammer, was domiciled in Austria and paid for the voyage. However, he later refused to embark as he claimed that the company's description of the voyage did not correspond to conditions on the vessel. As Reederei Karl Schlüter only reimbursed part of the sum paid, the claimant claimed payment of the balance before an Austrian court of first instance.

Hotel Alpenhof also concerned a consumer contract which gave rise to a dispute between the claimant, an Austrian hotel and a consumer resident in Germany. The consumer, Mr Heller, effected his reservation and confirmation by email. Having found

¹²⁰ The notion of directing one's activities to a specific country is analogous to the concept of 'targeting the public' in a particular country. The latter concept is analysed in depth in chapter 6 in the context of analysing the communication to the public right and its localisation in an online environment. On a different issue, advances in technology and e-commerce have enabled e-businesses to use geolocation technologies for content targeting. Through the use of geolocation technology, e-businesses are able to direct their websites to specific locations or particular Member States, thereby determining the reach of their website so as to avoid selected jurisdictions, see Bharat Saraf, Ashraf U Sarah Kazi, 'Analysing the application of Brussels I in regulating e-commerce jurisdiction in the European Union – Success, deficiencies and proposed changes' (2013) 29 Computer Law and Security Review 127, 134.

fault with the hotel's services, Mr Heller left the hotel without paying his bill. Hotel Alpenhof then brought an action before an Austrian court for payment of the sum owed. The ECJ stated that it should be ascertained whether before the conclusion of any contract with the consumer, it is apparent from those websites and the trader's overall activity that the trader was envisaging doing business with consumers domiciled in one or more Member States, including the Member State of that consumer's domicile, in the sense that it was minded to conclude a contract with them.¹²¹ The ECJ then set out a non-exhaustive list of matters which are capable of constituting evidence that the trader's activity is directed to the Member State of the consumer's domicile. The list includes the following:

the international nature of the activity, mention of itineraries from other Member States for going to the place where the trader is established, use of a language or a currency other than the language or currency generally used in the Member State in which the trader is established with the possibility of making and confirming the reservation in that language, mention of telephone numbers with an international code, outlay of expenditure on an internet referencing service in order to facilitate access to the trader's site or that of its intermediary by consumers domiciled in other Member States, use of a top-level domain name other than that of the Member State in which the trader is established, and mention of an international clientele composed of customers domiciled in various Member States. It is for the national courts to ascertain whether such evidence exists.¹²²

Factors deemed insufficient by the ECJ to show that a trader's activity is being directed to a certain Member State included: the mere accessibility of the trader's or the intermediary's website in the Member State in which the consumer is domiciled and, the mention of an email address and other contact details or the use of a language or a currency which are the language and/or currency generally used in the Member State in which the trader is established.¹²³

¹²¹ Joined cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG; Hotel Alpenhof GesmbH v Oliver Heller* [2010] ECR I-12527, para 92.

¹²² *Ibid* para 93.

¹²³ *Ibid* para 94.

This ruling is significant in that it helps to clarify the previously unclear jurisdictional concept of ‘directing activities’ to a particular country. As Rome I also contains the same concept (in Article 6(1)), the ruling has relevance for that regulation too. Clearly, the issue was considered of particular importance as the case was heard by a Grand Chamber. The decision to use a Grand Chamber may have been linked to the fact that the notion of ‘directing activities’ was the subject of intense debate by the various EU institutions and Member States during the legislative process, without a clear compromise being reached. As a consequence, the wording of Article 15 of Brussels I and Article 6 of Rome I was left deliberately vague and did not address the internet specifically. Ultimately, it was left to the CJEU to assume political responsibility for the interpretation of the notion.

2.11. The internet – bordered or borderless?¹²⁴

Technology is not the only way of raising borders on the internet. Countries such as China, Saudi Arabia, Iran and Myanmar apply strict controls (monitoring/censorship) to the internet¹²⁵ which may involve blocking access to material held on foreign servers. For instance, China’s State Council Information Office advocates a bordered internet based on territorial sovereignty.¹²⁶ This State-centred policy contrasts with the US State Department’s policy which holds that there be a single connected internet that is, to a degree, sovereign in its own right.¹²⁷ The American approach is more an individual-based, rights-centred, and market driven policy.

¹²⁴ For a general overview on the nature of the internet, - bordered or borderless?, see Bernhard Maier, ‘How has the law attempted to tackle the borderless nature of the internet?’ (2010) 18 IJLIT 142-175.

¹²⁵ See Nikolaos Koumartzis and Andreas Veglis, ‘Internet regulation: The need for more transparent internet filtering systems and improved measurement of public opinion on internet filtering’ (2011) 16 First Monday <<http://firstmonday.org/ojs/index.php/fm/article/view/3266/3071>> accessed 14 May 2014.

¹²⁶ Min Jiang, ‘Authoritarian Informationalism: China’s Approach to Internet Sovereignty’ (2010) 30 SAIS Review 71, 73.

¹²⁷ Ibid.

Unfortunately, China's adoption and promotion of the internet has gone hand in hand with its physical manipulation of internet architecture and control of internet use.¹²⁸ The Great Firewall of China, the world's most advanced national firewall, has blocked access to the following over the past five years: YouTube (blocked permanently in 2009), Facebook and Twitter (blocked since riots in Xinjiang in 2009), and Bloomberg and the New York Times (blocked in 2012, after publishing detailed reports on the finances of Chinese leaders' families).¹²⁹

Pervasive filtering also occurs in Saudi Arabia where a proxy system is used to block requests for banned websites. Most of the blacklisted sites are sexually explicit or about religion. But, even seemingly innocuous content about women's history and women's bathing suits is blocked.¹³⁰

Blocking is not just the preserve of developing or autocratic countries. Among developed countries, the UK's Cleanfeed system is a landmark model for large scale blocking. Created in 2003 by British Telecom in consultation with the UK Home Office, this system is aimed at blocking access to child sex abuse images. The blacklist of websites is compiled by the Internet Watch Foundation (IWF).¹³¹

¹²⁸ Ibid 75.

¹²⁹ 'The Great Firewall, The Art of Concealment' (*The Economist*, 6 April 2013) <<http://www.economist.com/news/special-report/21574631-chinese-screening-online-material-abroad-becoming-ever-more-sophisticated>> accessed 14 May 2014.

¹³⁰ See: OpenNet Initiative, 'Saudi Arabia' (2009) <<https://opennet.net/research/profiles/saudi-arabia>> accessed 14 May 2014.

¹³¹ A particularly compelling and slightly ironic example of censorship creep occurred in July 2011 when the English High Court in *Twentieth Century Fox Film Productions v British Telecommunications plc* ordered BT to block access to the Newzbin 2 website (The Pirate Bay) using the Cleanfeed system. See: Zack Whittaker, "'Censorship creep': Pirate Bay block will affect one-third of U.K.' (*CNET*, 16 June 2012) <http://news.cnet.com/8301-1023_3-57454683-93/censorship-creep-pirate-bay-block-will-affect-one-third-of-u.k/> accessed 14 May 2014. Incidentally, the *Twentieth Century Fox* ruling describes at [71] the three methods that ISPs can employ to block access to websites, namely, (i) DNS name blocking; (ii) IP address blocking using routers; and, (iii) Deep Packet Inspection-based URL blocking using ACLs on network management systems.

The UK's Cleanfeed system became the model for Canada's Project Cleanfeed which was rolled out in November 2006. The activities of Cleanfeed Canada, an undertaking of the Canadian Coalition Against Child Exploitation (CCAICE), demonstrates how borders can be erected in cyberspace. It *only* blocks customer access to non-Canadian websites which host child pornography. Suspect websites within Canada are investigated by Canadian law enforcement.¹³² Scandinavia, too, saw the implementation of a child pornography blocking system in October 2004. It involved the Norwegian telecoms company, Telenor, working in conjunction with KRIPOS (The Norwegian National Criminal Investigation Service).¹³³ One year later, Telenor was again instrumental in implementing another content blocking system, this time in Sweden.

2.12. Conclusions

One of the key problems for courts dealing with online torts is to localise the place where the act giving rise to the damage occurred, or the place where the damage itself occurred. Pinpointing the *locus delicti* has always been challenging, but in a border-disregarding, deterritorialised context such as the internet, the challenge is amplified.

The writings of Mann in 1964, demonstrate that the challenge of localisation is not new. Back then, however, his references were aimed at communications media now considered relatively unsophisticated e.g. the telephone, teleprinter, television and international advertising and the risk that trans-border distribution of content would too readily satisfy territorial connecting factors.

Sterling's description of the sequence of events comprising an online copyright infringement demonstrates the complexity involved. But, the analysis can be simplified by focusing on the two most significant acts in the whole chain – those of uploading and downloading. They are, in effect, the two constants in the whole equation.

As regards online defamation, the Australian High Court in *Dow Jones v Gutnick* considered the place of download as the *locus delicti*, rationalising that damage to

¹³² See generally: Canadian Centre for Child Protection Inc, 'Cleanfeed Canada' (*cybertip!ca*) <<https://www.cybertip.ca/app/en/projects-cleanfeed>> accessed 14 May 2014.

¹³³ Gert Vermeulen (ed), *EU quality standards in support of the fight against trafficking in human beings and sexual exploitation of children (Exploratory study of the potential and feasibility of self-regulation or public-private co-operation)* (Maklu 2007) 60.

reputation could only occur when/where the defamatory material was downloaded to the computer of the publishee who was then in a position to comprehend the defamation.¹³⁴ A similar approach, linking place of download with place of damage, occurred in the 2006 English High Court ruling *Ashton Investments Limited*¹³⁵ and this ruling was cited very recently by counsel in *Judith Vidal-Hall*,¹³⁶ a case concerning the online tort of breach of confidence.

In a practical deployment, the rule of upload is used in the Satellite Broadcasting and Cable Retransmission Directive, where communications to the public by satellite are localised in the Member State where the programme carrying signals are ‘uploaded’ to the satellite. In addition, there is the Scottish judgment - *Alan MacKie t/a 197 Aerial Photography v Nicola Askew, Llargsholidaylets.co.uk* – where the court betrayed a preference for place of upload when permitting the pursuer to choose between two jurisdictions in terms of initiating proceedings.¹³⁷ But, in granting the pursuer the option, the court was, in effect, following the principle laid down in *Bier v Mines de Potasse d’Alsace*,¹³⁸ whereby a plaintiff may sue in the courts of the place where the damage occurred, or in the courts of the place where the event giving rise to the damage occurred.¹³⁹

¹³⁴ *Dow Jones & Company Inc v Gutnick* [2002] HCA 56 [26] and [44].

¹³⁵ *Ashton Investments Ltd v OJSC Russian Aluminium (Rusal)* [2006] EWHC 2545 (Comm).

¹³⁶ *Judith Vidal-Hall and others v Google Inc* [2014] EWHC 13 (QB).

¹³⁷ *Alan MacKie t/a 197 Aerial Photography v Nicola Askew, Llargsholidaylets.co.uk* [2009] SLT (Sh Ct) 146 [28] et seqq.

¹³⁸ This ruling is dealt with in depth at para 4.2.3.2.

¹³⁹ Case 21/76 *Handelskwekerij GJ Bier BV v Mines de Potasse d’Alsace SA* [1976] ECR 1735, para 25.

Chapter 3. Transnational IP Infringement with Focus on Copyright

TABLE OF CONTENTS

3.1	The Objective of this Chapter	66
3.2	The proliferation of transborder copyright infringement.....	66
3.3	Essential elements needed in legal proceedings concerning copyright.....	69
3.4	Tensions between a deterritorialised internet and territorial IP	73
3.5	The UK	78
3.5.1	Lucasfilm Ltd v Ainsworth	78
3.6	Court of Justice of the European Union.....	81
3.6.1	Football Association Premier League Ltd v QC Leisure and Karen Murphy v Media Protection Services Ltd	81
3.6.2	Eva-Maria Painer v Standard VerlagsGmbH.....	85
3.6.3	Peter Pinckney v KDG Mediatech AG	86
3.6.4	Football Dataco Ltd v Sportradar	91
3.7	Conclusions	97

3.1 The Objective of this Chapter

The aim of this chapter is to provide some jurisprudential evidence that brings together three core elements of my research, namely, the internet, copyright (in particular, digital copyright) and PIL. Naturally, as the level of transborder copyright infringement increases, so does the likelihood of PIL issues arising. Cognisant of the sophisticated and harmonised system of PIL rules prevailing in the EU, I shall only treat UK or CJEU case-law in this chapter. I have included in this chapter treatment of the *Football Dataco*¹⁴⁰ ruling even though it relates to the database right. The fact that the case concerns Article 5(3) Brussels I and that the database right and copyright are proximate IPRs, constitute justification for the ruling's inclusion in this chapter.

This chapter will also demonstrate that much IPR infringement nowadays is internet-based and frequently these online torts have a transborder component. Clearly, the internet is not the only medium that facilitates infringement of digital copyright in a transborder context. Satellite and cable¹⁴¹ are also used to disseminate infringing digitised content and this is borne out by the ruling, *Football Association Premier League v QC Leisure*¹⁴² which is analysed later in this chapter.

Related themes are also explored in this chapter such as the tensions that exist between the deterritorialised internet and territorial IP and the way that the principle of territoriality creates a universal system of self-limitation of national substantive IP Law.

3.2 The proliferation of transborder copyright infringement

Without doubt, transnational copyright infringement has become much more frequent in the digital age.¹⁴³ Trade marks too, feature prominently among online IP

¹⁴⁰ Case C-173/11 *Football Dataco Ltd v Sportradar* [2013] CMLR 29.

¹⁴¹ The Satellite and Cable Directive is dealt with at para 5.4.1.

¹⁴² Joined Cases C-403/08 and C-429/08 *Football Association Premier League Ltd v QC Leisure; Karen Murphy v Media Protection Services Ltd* [2011] ECR I-9083, para 148.

¹⁴³ Clearly, all the principal IPRs are breached online. However, it seems to this author that copyright and trademark are subject to the highest rates of online infringement. Fawcett and Torremans provide useful examples of online infringements of the three main IPRs. James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 547 et seq. In addition, they list court rulings that reflect the examples given. As

infringements.¹⁴⁴ Statistics from China now point to a preponderance (60%) of copyright infringement among IP infringements during the first ten months of 2011 and to half of the copyright infringements having an online dimension.¹⁴⁵ Set against this backdrop of rising copyright infringement, it is not entirely surprising that cross-border copyright infringement has become significantly more commonplace thanks to such things as the internet, advances in Information Communication Technologies (ICT), the whole process of digitisation, and the desire (or strategy) of infringers or the facilitators of copyright infringement to base themselves outside the EU, in pirate havens, so as to try and avoid detection. However, the thing that sets the internet apart in this debate is its immense technical potential for communicating IP-protected works around the world. The internet has radically shaken up the IP world over the last fifteen years or so.

regards infringement of a patent online, the authors provide the following example: where a computer network user situated in France logs onto the network, accesses a machine that is physically situated in England, and runs software that would infringe an English patent. See Dan L Burk, 'Patents in cyberspace: Territoriality and infringement on global computer networks' (1993) 68 TLR 1, 39; James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) fn 90 et seq.

¹⁴⁴ Some good recent examples include the Adwords (or, Keywords) rulings from the CJEU to include Joined Cases C-236/08, C-237/08 and C-238/08 *Google France and Google Inc v Louis Vuitton Malletier*; *Google France v Viaticum Luteciel*; *Google France v CNRRH* [2010] ECR I-2417; Case C-323/09 *Interflora Inc, Interflora British Unit v Marks & Spencer plc, Flowers Direct Online Ltd* [2011] ECR I-8625; Case C-324/09 *L'Oréal SA v eBay International AG* [2011] ECR I-6011. These cases all feature one particular practice for which Google has become famous – of selling Adwords (or, keywords) which are identical or very similar to registered trade marks to traders who use those keywords for the purposes of promoting their own goods/services. The issue then arises: Are the following parties guilty of trade mark infringement - the service providers who sell the Adwords; the traders who purchase the Adwords; and, lastly, the internet search engines (e.g. Google) and online market places (e.g. eBay) whose services are used for the purpose of marketing infringing products? See generally, Christopher Morcom, 'Trade marks and the Internet: Where Are We Now?' (2012) 34 EIPR 40-53.

¹⁴⁵ These statistics were provided by the director of the third civil tribunal of China's Supreme People's Court in December 2011. Zhao Yinan, 'Online IPR infringement cases on the rise' (*China Daily*, 20 December 2011) <http://www.chinadaily.com.cn/china/2011-12/20/content_14294110.htm> accessed 24 June 2012.

These elements facilitate easy, immediate and widespread dissemination of digitised content. In addition, various other means of dissemination such as satellite broadcasting and cable (re)transmissions along with technological developments such as peer-to-peer file-sharing, streaming and linking all facilitate transborder transfers of copyright material. Given that a certain portion of this online activity will be unauthorised, it is almost inevitable that illegal transnational IP disseminations will occur. There seems to be a constant flow of case law and statistics from copyright-related sectors which indicate serious levels of digital copyright infringement. Many of these scenarios involve unauthorised dissemination of content such as text, data, music, pictures, graphics and film on the internet. Clearly, this is the stuff of copyright litigation. The fact that names and terms such as Napster, Gnutella, FastTrack, Kazaa, peer-to-peer (or, file-sharing), and Bit-Torrent have become household names over the past decade or so demonstrates clearly how copyright has featured prominently in terms of internet IP infractions. In fact, Fawcett and Torremans, citing Ginsburg opine that IP infringement over the internet is *most likely* to arise in cases of breach of copyright.¹⁴⁶

Besides the prominent case of illegal file-sharing, other entities like YouTube (video-sharing), LinkedIn (business network), MySpace (social networking), Facebook (social networking), and Twitter (social messaging tool) revolve around copyright-protected material. In fact, YouTube's commercial existence/survival depends on copyright material. It is one of life's realities that some of the copyright content featuring in the aforementioned media are used without copyright holder approval and sometimes disseminated cross-border.¹⁴⁷

¹⁴⁶ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) para 10.40; Jane Ginsburg, 'Putting Cars on the Information Superhighway: Authors, Exploiters and Copyright in Cyberspace' (1995) 95 Colum L Rev 1466, fn 84.

¹⁴⁷ Under proposals set out in the Hargreaves Report, a modernised system of licensing has been mooted. This new system would be operated by a Digital Copyright Exchange which would establish a network of interoperable databases to provide a common platform for licensing transactions. Licensing across delivery technologies would also be accommodated by the new body. Ian Hargreaves, 'Digital Opportunities – A Review of Intellectual Property and Growth' (May 2011) para 4.31 <<http://www.ipo.gov.uk/ipreview-finalreport.pdf>> accessed 24 June 2012. Certain key benefits would flow from the proposed Exchange, eg from the creator's perspective: a clearer understanding of licensing terms and conditions throughout

Arguably worse is to come for digital copyright holders as Web 2.0, the participatory Web, promises much more interaction and user-created content. Having a close association with participatory information sharing, Web 2.0 facilitates interoperability, user-centred designs and collaboration on the WWW. Examples of Web 2.0 include social networking sites, blogs, wikis, video sharing sites, hosted services, web applications, mashups and folksonomies.

In the context of Web 2.0, new IT tools will facilitate the creation of new works. Frequently, these will be derivative works, based on existing IP protected works that will be transformed in a more or less radical or comprehensive way. The upshot will be a set of even more complex IP issues especially as there will almost inevitably be more contributors in the transformation chain, in even more different jurisdictions.¹⁴⁸

3.3 Essential elements needed in legal proceedings concerning copyright

To establish a framework for critical review of court rulings with a transnational copyright element (treated later in this chapter) and for later chapters, I shall now set out the necessary elements.

As a practical matter, in order for a court definitively to rule on a copyright dispute (whether in favour of the claimant or defendant), the following elements are needed. They are basically the same for offline and online infringement, but when they span more than one jurisdiction, the three pillars of PIL come into play. This complexity is compounded by the geographical uncertainties of infringement on the internet.

the market and increased options to license an individual creator's works directly; from the intermediary right holder's perspective: automated licensing via standard terms if offered by the rights holder and, decreased risk of infringements by providing clarity as to what is licensed and what is not via terms checkable at the click of a mouse; and, lastly, from the consumer's perspective: a place where those seeking to use copyright works can quickly identify the right holder and secure a licence, either through automation or via a negotiating agent.

¹⁴⁸ James J Fawcett and P Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) para 10.04.

1. A claimant with legal capacity and standing to sue

The Berne Convention ensures that an original work will be protected in most countries in the world. However, the claimant must demonstrate that it has an appropriate interest in the relevant copyright(s). For example, in the UK, the owner of the rights may sue,¹⁴⁹ an exclusive licensee of the relevant rights,¹⁵⁰ and, in limited circumstances, a non-exclusive licensee.¹⁵¹

The Berne Convention requires protection for authors and their works; it does not, however, govern rules on transfer and ownership. These questions, and indeed which law applies in ascertaining the answers, are left to contracting states. The Max Planck CLIP¹⁵² proposal seeks to settle this in Article 2:205 (jurisdiction over entitlement and ownership), Article 3:201 (choice of law on initial ownership), and Article 3:301 (choice of law on transferability). The ALI proposals¹⁵³ allow the law of each country for which the rights are exercised to determine transferability (Section 314), but tie initial ownership to the country where the creator was resident when the work was created (Section 313(1)(a)).¹⁵⁴

It will be assumed that the legal capacity of the claimant is not a problem.

¹⁴⁹ CDPA 1988, s 96.

¹⁵⁰ *Ibid* s 101.

¹⁵¹ *Ibid* s 101A.

¹⁵² The Max Planck Group on Conflict of Laws in Intellectual Property was established in 2004. The Group drafted a set of principles on conflict of laws in IP and advanced the Final Text of the Principles on 31 August 2011 at a conference on the CLIP Principles in November 2011 at the Harnack-Haus in Berlin.

¹⁵³ ALI, *Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes* (ALI Publishers 2008).

¹⁵⁴ Section 313(1)(a) states that the initial title to IPRs that do not arise out of registration will be governed by the law of the creator's residence at the time the subject matter was created.

2. A defendant with legal capacity on whom liability may be imposed, directly or indirectly

The problem of minors downloading material in an unauthorised way has exercised legislatures (European Parliament), copyright holders, and commentators.¹⁵⁵ Again it will be assumed in this thesis that the defendant has legal capacity. Arguments as to indirect or contributory infringement may be raised against internet service providers, the providers of file-sharing software etc.

3. A court with jurisdiction over the defendant and subject-matter

Jurisdiction over a defendant may be personal (defendant's domicile – Article 2, Brussels I), based on the fact of multiple defendants (Article 6, Brussels I), or derived from subject-matter jurisdiction (e.g. place of harmful event – Article 5(3), Brussels I) or, occasionally, based on the possession of assets in the jurisdiction (e.g. Germany, by virtue of Article 23, Code of Civil Procedure of Germany).¹⁵⁶ Locating and identifying the defendant is crucial – ‘John Doe’ litigation and roving *Anton Piller* orders are problematic in the offline world, let alone online.

Subject-matter jurisdiction may be direct or related to personal jurisdiction (e.g. under Brussels I, the court of the defendant's domicile may confer subject-matter jurisdiction for the whole EU). In addition, there may be *lis pendens* rules preventing multiple assumptions of jurisdiction (e.g. Articles 27 and 28, Brussels I).¹⁵⁷

4. A cause of action for copyright infringement

This will depend upon the applicable law, but will comprise at least acts restricted by copyright, relevant geographical connections and lack of consent.

¹⁵⁵ William Patry, ‘Can a Minor be Sued for Infringement?’ (*The Patry Copyright Blog*, 28 September 2006) <<http://williampatry.blogspot.co.uk/2006/09/can-minor-be-sued-for-infringement.html>> accessed 15 August 2012.

¹⁵⁶ ‘The Brussels I Regulation (No 44/2001)’ (*Dutch Civil Law*) <<http://dutchcivillaw.com/content/brusselone022.htm>> accessed 15 August 2012.

¹⁵⁷ See para 4.2.6.

5. Exceptions and limitations

These depend critically upon the applicable law, as witness the closed but non-mandatory set in Article 5 of the InfoSoc Directive.

6. Law applicable to substantive issues

7. Evidence

This must be admissible and persuasive under relevant procedural law to establish commission of infringement (presumptions may be available under international and local law) and any exceptions/limitations relied upon.

8. Availability of remedies

This is a matter decided by the substantive law. A case in point is *Lucasfilm Ltd v Ainsworth*.¹⁵⁸ In 2006, the US District Court (Central District of California) awarded Lucasfilm \$20 million by way of default judgment. However, the whole judgment went unsatisfied right up to the English Supreme Court's ruling in July 2011. While the Supreme Court held that it could assume jurisdiction over the case (provided it had *in personam* jurisdiction over the defendant), it made no statement on its attitude to US statutory damages. However, conceivably, an English court could award a much lower figure than that awarded by the Californian court if, under the pre-Rome II rules,¹⁵⁹ it were to apply English procedural law when quantifying the damages.¹⁶⁰ Going forward, one cannot entirely rule out the possibility of US style damages awards in the EU as

¹⁵⁸ *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39.

¹⁵⁹ Private International Law (Miscellaneous Provisions) Act 1995, s 14 (3), *Boys v Chaplin* [1971] AC 356; *Harding v Wealands* [2006] UKHL 32.

¹⁶⁰ Daniel Hart, 'Star Wars Episode III – English Supreme Court decision: A New Hope for the enforcement of non-EU copyrights, or a Phantom Menace for UK-domiciled entities?'

(*Mayer Brown*, 13 September 2011) 4

<<http://www.mayerbrown.com/files/Publication/66ac2a8d-59e2-4df4-b9a2-63a0190fd2f2/Presentation/PublicationAttachment/e687d1a6-f0f9-4c52-af8c-795d4509b1ad/11551.pdf>> accessed 23 August 2012.

Rome II provides that a foreign law governing a non-contractual claim will also apply to the quantification exercise.¹⁶¹

9. Means of enforcement of remedies

This is usually regarded as the third pillar of PIL, after jurisdiction and applicable law. However its availability or non-availability may be a relevant factor in a court's assuming or declining jurisdiction. Recent case-law, involving infringements on- and offline will be analysed within this framework, and subsequent chapters will investigate whether and how various elements may be established.

3.4 Tensions between a deterritorialised internet and territorial IP

One obvious tension that exists is that between the non-territorial (or, deterritorialised) internet and the territorial nature of IP.¹⁶² The territoriality principle holds that the IP laws of one country only apply within that country. As Ginsburg and Lucas note:

¹⁶¹ Sarah Byrt and Daniel Hart, 'Copyright Across Borders' in Mayer Brown, 'Expert Guide: Intellectual Property' (*Corporate Live Wire*, December 2011) 17
<http://www.mayerbrown.com/files/News/766c77f9-5f13-478c-aec1-17ecc831941e/Presentation/NewsAttachment/59ac67c0-42c9-458d-9fad-1bbca7f87dda/ART_BYRT_HART_DEC11_COPYRIGHT-ACCROSS-BORDERS.PDF> accessed 23 August 2012, referring to Article 15, Rome II, which states that the law applicable to a non-contractual obligation shall govern (among other things) the existence, the nature and the assessment of damages or the remedy claimed.

¹⁶² Peukert describes intellectual property law as 'probably one of the most "territorial" branches of commercial law. Alexander Peukert, 'Territoriality and Extraterritoriality in Intellectual Property Law' (*SSRN*, 19 April 2010) 36
<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1592263> accessed 31 May 2014. Rotstein refers to 'the core principle of territoriality that informs so much of the international intellectual property system. Fiona Rotstein, 'Is there an international intellectual property system? Is *there* an agreement between states as to what the objectives of intellectual property should be?' (2011) 33 *EIPR* 1, 4. David Vaver states that 'Copyright law is territorial, so in principle only one country's law should apply to a single act, and users should not be liable to overlapping laws.' David Vaver, 'Recent Copyright Law Developments Reform?' (2010) 22 *IPJ* 1, 9.

‘Each country determines, for its own territory and independently from any other country, what is to be protected as intellectual property, who should benefit from such protection, for how long and how protection should be enforced.’¹⁶³

In effect, under the territoriality principle, foreign rights cannot be infringed by local activity and local rights cannot be infringed by foreign activity.¹⁶⁴ As regards UK copyright, Section 16(1) of CDPA 1988 contains a clear rule concerning the territorial scope. For UK Copyright Law to apply, the infringing acts must take place in the UK.¹⁶⁵ This rule has been followed in a line of cases to include the rulings in *Jonathan Cape Ltd v Consolidated Press Ltd* [1954],¹⁶⁶ *Def Lepp Music v Stuart Brown* [1986],¹⁶⁷ and *Atkinson Footwear Ltd v Hodgkin International Services Ltd* [1995].¹⁶⁸ The key element is that the infringing copies are actually made in the UK. If they are illegally reproduced in the UK with the sole aim of exporting them to foreign countries, the exportation element will be irrelevant. The reproductions will still be deemed illegal under UK Copyright Law because of the place of reproduction.¹⁶⁹ As an extension of this rule, illegal reproductions made outside the UK on the basis of an authorisation given in the

¹⁶³ Jane C Ginsburg and André Lucas, ‘The Role of Private International Law and Alternative Dispute Resolution in WIPO, Intellectual Property on the Internet: A Survey of Issues’ (WIPO/INT/02, 2002) para 283.

¹⁶⁴ See German Bundesgerichtshof (Federal Court of Justice) rulings in the following cases: BGHZ 41, 84 (15) (‘Maja’); BGHZ 49, 331 (20) (‘Vorán’); IIC 1977, 276 (278) (‘Hummel Christmas Plate’); IIC 1995, 573 (575) (‘Folgerecht’).

¹⁶⁵ This situation seems to have changed following the recent ruling in *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39 in which the UK Supreme Court held that provided there is a basis for *in personam* jurisdiction over the defendant, it would have jurisdiction to hear a case where the unauthorised reproduction and sale by the defendant occurred in the US, not the UK. UK Patents Law has a provision very similar to CDPA 1988, s16(1). It is Patents Act 1977, s 60 which clearly restricts infringing acts to acts committed in the UK. Oddly, the UK’s Trade Marks Act 1994 does not contain a territorial restriction but this seems more of a legislative oversight than anything else. There is nothing in the Trade Marks Act 1994 to indicate that the British Parliament was attempting to rule extra-territorially as well!

¹⁶⁶ *Jonathan Cape Ltd v Consolidated Press Ltd* [1954] 1 WLR 1313.

¹⁶⁷ *Def Lepp Music v Stuart-Brown* [1986] RPC 273.

¹⁶⁸ *Atkinson Footwear Ltd v Hodgkin International Services Ltd* (1995) 31 IPR 186.

¹⁶⁹ A similar rule prevails under Dutch Copyright Law. See, eg *NV Gebr Van Zijverden v GF Mens* [1973] BIE 99.

UK, will still fall outside UK Copyright Law due to the place of reproduction. Only an authorisation to perform an infringing act *in the UK* will be actionable under UK Copyright Law.¹⁷⁰

EU jurisprudence and legislation have also confirmed the territoriality principle. In *Lagardère Active Broadcast v SPRE and GVL*, a case involving a royalties-related dispute between a broadcaster (Lagardère Active Broadcast) and two collecting agencies (SPRE and GVL), the European Court of Justice stated as follows:

the principle of the territoriality of those rights, which is recognised in international law and also in the EC Treaty. Those rights are therefore of a territorial nature and, moreover, domestic law can only penalise conduct engaged in within national territory.¹⁷¹

In terms of EU legislation, the application of a foreign IP Law is excluded under the Electronic Commerce Directive.¹⁷² This occurs by virtue of Article 3(3) which states

¹⁷⁰ See *ABKCO Music & Records Inc v Music Collection International Ltd* [1995] RPC 657, 660 (Hoffmann LJ). A similar rule exists in US Copyright Law, see *Subafilms Ltd v MGM-Pathe Communications Co*, 24 F 3d1088 (9th Cir 1994).

¹⁷¹ Case C-192/04 *Lagardère Active Broadcast v Société pour la perception de la rémunération équitable (SPRE) and Gesellschaft zur Verwertung von Leistungsschutzrechten mbH (GVL)* [2005] ECR I-7199, para 46. This case concerned rental and lending rights (Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property [1992] OJ L346/61) and rights related to copyright applicable to satellite broadcasting and cable retransmission (Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15). The ruling was a Preliminary Ruling following a request made by the French Court de Cassation (Supreme Court). The transnational component arose because Lagardère (established in France) transmitted signals to a satellite, which, in turn, transmitted to a transmitter in Felsberg (Germany). The Felsberg transmitter was technically equipped to broadcast to France on long wave (and this was carried out by Lagardère's subsidiary, Europe 1).

¹⁷² Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on Electronic Commerce) [2000] OJ L178/1, art 3(3).

that the country of origin rule does not apply to IPRs. The principle of territoriality is also safeguarded at multilateral convention level. Both the Berne Convention (1886) and the Paris Convention (1883) adhere to the principle of national treatment according to which each Contracting State accords the rights provided for in the conventions to nationals of other Contracting States. Thus, international law in the field of IP confirms that IP protection is limited territorially and personally. Given that there are currently 175 Contracting States of the Paris Convention¹⁷³ and 167 Members/Contracting States of the Berne Convention,¹⁷⁴ it is safe to say that objective¹⁷⁵ and subjective territoriality¹⁷⁶ are universally accepted concepts.¹⁷⁷

¹⁷³ WIPO, 'Contracting Parties Paris Convention'

<http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=2> accessed 29 May 2014.

¹⁷⁴ WIPO, 'Contracting Parties Berne Convention'

<http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15> accessed 29 May 2014.

¹⁷⁵ The objective dimension of the territoriality principle refers to the fact that an IP right is limited to the territory of the State granting it. The exclusive right can only cover activities occurring within the respective territory. Things which are capable of copyright protection are subject to a bundle of possibly more than 150 territorial rights of national or regional provenance. These rights are independent from each other so that a work may be protected in one country but unprotected in another. There are as many property legislations as there are IP rights. A comparative survey reveals that this objective territoriality principle has long been accepted by the EU, its Member States like Germany or the Netherlands, other European countries like Switzerland, common law countries around the globe, Japan and the US. Alexander Peukert, 'Territoriality and Extraterritoriality in Intellectual Property Law' (SSRN, 19 April 2010) 1 et seq, fn 2-13

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1592263> accessed 31 May 2014.

¹⁷⁶ Since the territorially limited rights are independent from one another, they may be owned by different persons, even if the same subject matter is concerned. National legislation may not only grant the rights in the same work to different persons, it may also restrict the availability of protection to its nationals and extend it to foreigners only under certain conditions, in particular by way of local publication/production or reciprocity requirements. This state of affairs is known as subjective territoriality. Ibid 3.

¹⁷⁷ Ibid 4.

From a conflicts perspective, one important effect of the principle of territoriality is that it creates a universal system of self-limitation of national substantive IP Law. This element of self-limitation affects the normal operation of the choice-of-law process. Since all possible applicable laws are limited to a territory and none is universal in scope, none can apply in another territory. The logical follow-on according to Peukert is that only the law of the country for which protection is sought (*lex loci protectionis*), also considered to be most closely related to the issue, will determine whether a right exists, whether it has been infringed, and most general aspects concerning the IPR. The Rome II Regulation¹⁷⁸ bolsters the status of the *lex loci protectionis* by stating that the principle is ‘universally acknowledged’ and that it ‘should be preserved’.¹⁷⁹ The principle is actually enshrined in Article 8(1), Rome II. The territoriality principle signifies a mosaic of independent, territorially and personally limited exclusive rights to be applied by local courts.

As the internet is ubiquitous or global in nature, it tends to cross *all* national borders. Its ubiquity ensures that it is not particularly dependent on national borders. Nor is it circumscribed by them. These facts virtually guarantee that it will come into conflict with IP which is strongly based on the territoriality principle. Somewhat ironically too, the internet’s virtual global presence combined with its all-pervasiveness means that it is the perfect and natural medium to accommodate trans-national, multi-state IP infringement.

It is important to acknowledge in this section of the thesis that the territoriality principle is gradually being diluted by the internet and an increasingly global exploitation of rights. Viewing territoriality from the perspective of choice of law, Rotstein lists off the various approaches she describes as alternatives to territoriality: the US ‘root copy’ approach, the ‘nerve centre’ approach, the law of the author’s country of residence or place of business, i.e. the place where the harm is ultimately felt, the *lex fori* and the *lex mercatoria* (for cyberspace).¹⁸⁰

¹⁷⁸ See para 5.2.1.

¹⁷⁹ Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L 199/40, recital (26).

¹⁸⁰ Fiona Rotstein, ‘Is there an international intellectual property system? Is there an agreement between states as to what the objectives of intellectual property should be?’ (2011) 33 EIPR 1, 4.

In an endeavour to demonstrate just how common transborder copyright infringements are, the author devotes the second half of this chapter to analysing a number of rulings from both the UK and the CJEU.

I will start my analysis with *Lucasfilm*, handed down by the UK's Supreme Court and then move onto the CJEU rulings.

3.5 The UK

3.5.1 *Lucasfilm Ltd v Ainsworth*¹⁸¹

One of the key issues raised in this appeal from the Court of Appeal ruling (2009) was whether an English court could exercise jurisdiction in a claim against persons domiciled in England for copyright infringement committed outside the EU in breach of copyright law of that country.

The case revolved around alleged breach of artistic works associated with the Star Wars film, more specifically, with unauthorised reproduction and sale by Ainsworth in the US of the Imperial Stormtrooper helmets. Ainsworth sold \$30,000 worth of the goods in the US. Lucasfilm obtained judgment against him in the US. It also commenced proceedings in the English courts, including claims for infringement of English copyright and claims under US Copyright.

While this Supreme Court ruling from July 2011 raised two distinct issues, the justiciability issue is the one that is of most relevance to this thesis.¹⁸² On the issue of justiciability, the Supreme Court overruled the Court of Appeal. It held that provided there is basis for *in personam* jurisdiction over the defendant, an English court does have jurisdiction to try a claim for infringement of copyright of a kind involved in the present action.¹⁸³ At an earlier stage in the proceedings, the Court of Appeal ruled that the common law rule in *British South Africa Co v Companhia de Moçambique*¹⁸⁴ was in

¹⁸¹ *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39.

¹⁸² The other issue is related to the definition of 'sculpture' in the CDPA 1988 and, in particular, the correct approach to three-dimensional objects that have both an artistic purpose and a utilitarian function.

¹⁸³ *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39 [106].

¹⁸⁴ *British South Africa Co v Companhia de Moçambique* [1893] AC 602.

fact an example of a general principle which applied to claims for infringement of foreign IPRs.¹⁸⁵ In *Companhia de Moçambique*, an English court was held not to have jurisdiction to entertain an action for determination of title to, or the right of possession of, foreign land, or the recovery of damages for trespass to such land.¹⁸⁶ The respondents (Ainsworth et al) argued that the *Moçambique* rule (as extended in *Hesperides Hotels Ltd v Muftizade*¹⁸⁷) still subsisted and applied to claims for infringement of all foreign IPRs including copyright because such claims are essentially ‘local’ and must be brought in the place where the rights have been created, irrespective as to whether there is any claim to title.¹⁸⁸

The Supreme Court rejected the respondents’ argument and found the claim justiciable. The court drew attention to the fact that much of the underpinning of the *Moçambique* rule and the decision in *Potter v Broken Hill Pty Co Ltd*¹⁸⁹ had been eroded and the rule in *Phillips v Eyre*¹⁹⁰ is gone.¹⁹¹

¹⁸⁵ *Lucasfilm Ltd v Ainsworth* [2009] EWCA Civ 1328 [175].

¹⁸⁶ *British South Africa Co v Companhia de Moçambique* [1893] AC 602.

¹⁸⁷ *Hesperides Hotels Ltd v Muftizade* [1979] AC 508.

¹⁸⁸ *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39 [105].

¹⁸⁹ *Potter v Broken Hill Pty Co Ltd* [1905] VLR 612, affd [1906] 3 CLR 479. Potter is an influential decision which is generally regarded as extending the *Moçambique* rule to actions for patent infringement. Potter obtained a patent in Victoria for the separation of metals from sulphide ores and a patent for the same process in New South Wales. Potter claimed a threatened infringement of the Victorian patent in Victoria and an infringement by the defendant company of its New South Wales patent at its mine in New South Wales. Broken Hill argued that an action for the infringement in New South Wales of a New South Wales patent was not justiciable in the Victorian courts. The Full Court of the Supreme Court of Victoria held that the claim was not justiciable and an appeal to the High Court of Australia was dismissed. *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39 [61].

¹⁹⁰ *Phillips v Eyre* [1870] LR 6 QB 1. The rule in *Phillips v Eyre* was generally known as the rule of double-actionability. It stipulated that as a general rule, to found suit in England for a tort alleged to have been committed abroad, two conditions had to be satisfied: (i) the alleged wrong must have been actionable as a tort if committed in England; and (ii) the act must not have been justifiable by the law of the place where it was done (the act had to be actionable in the place where it was committed). The rule was gradually eroded by case-law (*Boys v Chaplin* [1971] AC 356; *Red Sea Insurance Co Ltd v Bouygues SA* [1995] 1 AC 190) and finally abolished by the Private International Law (Miscellaneous Provisions) Act 1995.

Nor could the Supreme Court see any scope for the application of the act of state doctrine¹⁹² in this case. Instead, it highlighted the fact that the modern trend is in favour of the enforcement of foreign IPRs. In this regard, the court gave three examples of the modern trend. Firstly, Article 22(4) of Brussels I only assigns *exclusive* jurisdiction to the country where the right originates in cases which are concerned with registration or validity of rights which are ‘required to be deposited or registered’.¹⁹³ As copyright is rarely if ever deposited or registered (the US being an exception), situations of exclusive jurisdiction will be exceptionally rare and the likelihood of local courts assuming jurisdiction over foreign copyright infringements will remain a distinct possibility. Secondly, the Rome II Regulation plainly envisages the litigation of foreign IPRs.¹⁹⁴ And, thirdly, the professional and academic bodies which have considered the issue – the American Law Institute and the Max Planck Institute – clearly favour the enforcement of foreign IPRs.¹⁹⁵ Besides this modern trend, the Supreme Court also

¹⁹¹ *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39 [106], [108].

¹⁹² In the US, the act of state doctrine has been used as a basis for non-justiciability of foreign trade marks and patent rights. In the 1956 ruling, *Vanity Fair Mills, Inc v T Eaton Co Ltd*, 234 F 2d 633, 646 (2d Cir 1956), 352 US 871 (1956), the Court of Appeals for the Second Circuit held that a US federal court should not rule on the validity of a Canadian trade mark because (among other reasons) the act of state doctrine precluded determination of the acts of a foreign sovereign done within its own territory, and to rule on validity would create conflicts with Canadian administrative and judicial officers. The act of state doctrine was invoked more recently in the US as a ground for refusing to allow the addition of claims for infringement of parallel foreign patents to claims for infringement of US patents in litigation in which validity was in issue. See: *Voda v Cordis Corp*, 476 F 3d 887 (Fed Cir 2007).

¹⁹³ *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39 [109].

¹⁹⁴ *Ibid*.

¹⁹⁵ *Ibid* [94] et seq, [109]. The ALI’s *Intellectual Property: Principles Governing Jurisdiction, Choice of Law and Judgments in Transnational Disputes* (ALI Publishers 2008) are referred to in the judgment at [94] as applying to transnational civil disputes which involve IPRs. Section 211 provides that the court must have subject-matter and personal jurisdiction. The judgment also refers at [95] to draft principles prepared by the EU Max Planck Group on Conflict of Laws in IP. While these draft Principles contain no specific provision for actions for infringement of foreign rights abroad, it is implicit in the Principles that they envisage such actions. Within the Principles, the primary law applicable to infringement is the law of the State for which protection is sought. European Max Planck Group, Principles for Conflict

justified its assumption of jurisdiction in this case by referring to the frequent grant in the UK of extra-territorial injunctions against defendants subject to *in personam* jurisdiction. The Supreme Court was also quick to dismiss the lack of an international regime for the mutual recognition of copyright jurisdiction and of copyright judgments as a reason for it to refuse to take jurisdiction over an English defendant in a claim for breach of foreign copyright.¹⁹⁶ Two years earlier, the Court of Appeal had relied on this fact to decline jurisdiction in the case.¹⁹⁷

Finally, another interesting aspect of *Lucasfilm* is the Supreme Court's analysis of the issue of justiciability (in foreign copyright infringement cases) in other common law jurisdictions. It found that in both New Zealand (High Court)¹⁹⁸ and South Africa (Supreme Court of Appeal),¹⁹⁹ claims for infringement of foreign copyright were held to be non-justiciable. However, in a later High Court of New Zealand ruling, *KK Sony Computer Entertainment v Van Veen*,²⁰⁰ that court held that a claim for infringement of foreign IPRs (in that case, breach of UK and Hong Kong copyright in PlayStation 2) was justiciable if no question of the existence or validity of those rights was in issue.²⁰¹

3.6 Court of Justice of the European Union

3.6.1 *Football Association Premier League Ltd v QC Leisure and Karen Murphy v Media Protection Services Ltd*

This case is in fact a preliminary ruling under Article 267 TFEU,²⁰² following references from the English High Court (both, Chancery Division and Queen's Bench Division).

of Laws in Intellectual Property, The Draft (*Max-Planck-Gesellschaft*, 25 March 2011) 19-21 <<http://www.cl-ip.eu/files/pdf2/draft-clip-principles-25-03-20117.pdf>> accessed 12 July 2012.

¹⁹⁶ *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39 [88] et seqq.

¹⁹⁷ *Lucasfilm Ltd v Ainsworth* [2009] EWCA Civ 1328 [174], [183].

¹⁹⁸ *Atkinson Footwear Ltd v Hodgskin International Services Ltd* (1994) 31 IPR 186 (Tipping J).

¹⁹⁹ *Gallo Africa Ltd v Sting Music (Pty) Ltd* [2011] 1 All SA 449 (SCA).

²⁰⁰ *KK Sony Computer Entertainment v Van Veen* (2006) 71 IPR 179 (MacKenzie J).

²⁰¹ *Lucasfilm Ltd v Ainsworth* [2011] UKSC 39 [101].

²⁰² Consolidated Version of the Treaty on the Functioning of the European Union [2008] OJ C115/47; Consolidated Version of the Treaty establishing the European Community (TEC)

The case is interesting in that it deals with the delicate interface between IP and satellite broadcasting. It also looks at IP in the context of the Information Society.

In this case, the transnational copyright element arose in the context of satellite broadcasts (encrypted audiovisual content) of Premier League football matches from Greece which were accessed in the UK through the (allegedly unauthorised) use of a Greek card and decoder box.²⁰³ In terms of the essential elements needed before a court can rule on a copyright dispute, discussed earlier in this chapter, the cause of action for copyright infringement stands out in this case. Briefly put, the cause of action derived from the breach of Article 3(1) of the InfoSoc Directive by the owners of the public houses. This infringement of the communication to the public right²⁰⁴ provided a cause of action to the two main rightholders - FAPL and Multichoice Hellas (the Greek broadcaster).

The original copyright work is produced by the FAPL when it films Premier League matches. Subsequently, logos, video sequences, on-screen graphics, music and English commentary are added at a production facility. A new copyright is created when the signal is sent by satellite to a broadcaster which adds its own logos and possibly some commentary. In the instant case, that second broadcaster (or holder of the sub-licence) was the Greek entity NetMed Hellas. The ruling acknowledges that 'two categories of persons can assert intellectual property rights relating to television broadcasts - firstly, the authors of the works concerned (i.e. FAPL) and, secondly, the broadcasters (such as Multichoice Hellas).²⁰⁵

[2002] OJ C325/33.

²⁰³ The broadcasting was set up on the basis of territorial exclusivity. FAPL exercised the television broadcasting rights by granting exclusive (three year) licences to foreign broadcasters. Those broadcasters were required under their licence agreement with FAPL to ensure that their broadcasts which were capable of being received outside their exclusive licence territory were encrypted. In this case, the Greek sub-licensee was NetMed Hellas which broadcast the matches on SuperSport Channels on the NOVA platforms, owned and operated by Multichoice Hellas. The UK licensee was BSkyB Ltd.

²⁰⁴ See para 6.10.

²⁰⁵ Joined Cases C-403/08 and C-429/08 *Football Association Premier League Ltd v QC Leisure; Karen Murphy v Media Protection Services Ltd* [2011] ECR I-9083, para 148.

The right that was ultimately held to have been infringed was the communication to the public²⁰⁶ within the meaning of Article 3(1) of the InfoSoc Directive.²⁰⁷ Article 3(1) gives authors the *exclusive right* to authorise or prohibit any communication to the public of their works by wire or wireless means.²⁰⁸

The CJEU referred to one of its previous rulings in *Sociedad General Autores y Editores de España (SGAE) v Rafael Hoteles SA*²⁰⁹ where a hotel proprietor was deemed to have carried out an act of communication when he gave his customers access to the broadcast works via television sets, by distributing in the hotel rooms, the signal received carrying the protected works. It was pointed out by the court that such an act (intervention) was necessary for customers to be able to enjoy the broadcast works.

The court drew the analogy between *FAPL v QC Leisure* and *Rafael Hoteles*. In the former, the owner of a public house intentionally gave the customers present access to a broadcast containing protected works via a television screen and speakers. Without his intervention, the customers could not enjoy the works broadcast even though they were physically within the broadcast's catchment area.²¹⁰

However, when considering whether an infringement has occurred under Article 3(1) of the InfoSoc Directive, it is important to ascertain whether the work broadcast was transmitted to a *new* public, that is, to a public which was not taken into account by the

²⁰⁶ See para 6.10.

²⁰⁷ Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10 is referred to in short as the InfoSoc Directive.

²⁰⁸ This chapter will not treat in depth the reproduction right and the related acts of reproduction which were performed within the memory of the satellite decoder and on a TV screen as they were held to fulfil the conditions laid down in Article 5(1) of the InfoSoc Directive (the exceptions and limitations provision) and may therefore be carried out without the authorisation of the copyright holders concerned. In other words, such acts of reproduction were found to be non-infringing by the CJEU.

²⁰⁹ Case C-306/05 *Sociedad General Autores y Editores de España (SGAE) v Rafael Hoteles SA* [2006] ECR I-11519.

²¹⁰ In *Rafael Hoteles*, the hotel intervenes to give access to the protected work to its customers. In the absence of that intervention, the hotel's guests (although physically within the hotel) would not have been able to enjoy the broadcast works. *Ibid* para 42.

authors of the protected works when they authorised their use by the communication to the original public.

In the present case, when the Greek broadcasters authorised a broadcast of their works, they considered principally the owners of TV sets who either personally or within their own private or family circles received the signal and followed the broadcasts. But, where a broadcast work is transmitted in a place accessible to the public for an additional public which is permitted by the owner of the TV set to hear or see the work, then an intentional intervention of that kind must be regarded as an act by which the work in question is communicated to a *new* public.

Such a situation transpires when broadcast works are transmitted by the owner of a public house to the customers present in the establishment because those customers constitute an additional public which was not considered by the authors when they authorised the broadcasting of their works.

The court also attached importance to the fact that the relevant communication was of a profit-making nature. In the court's view, it was indisputable that the proprietor transmitted the broadcast works in his public house in order to benefit therefrom and that the transmission was liable to attract customers. The natural consequence of all this was that the transmission in question had an effect upon the number of people going to the establishment and ultimately on its financial results.

Weighing up all the foregoing points, the CJEU ruled that 'communication to the public' within the meaning of Article 3(1) must be interpreted as covering transmission of the broadcast works, via a TV screen and speakers, to the customers present in a public house.²¹¹ The implication there is that UK public houses which wish to screen live Premier League matches may only do so by obtaining the prior permission of the copyright owner.

²¹¹ Joined Cases C-403/08 and C-429/08 *Football Association Premier League Ltd v QC Leisure; Karen Murphy v Media Protection Services Ltd* [2011] ECR I-9083, para 207.

3.6.2 *Eva-Maria Painer v Standard VerlagsGmbH*

Another CJEU case involving transnational copyright infringement (albeit offline in nature) is that of *Eva-Maria Painer v Standard VerlagsGmbH*.²¹² It is, in fact, a preliminary ruling under Article 267 TFEU, delivered on 1 December 2011.²¹³

This case involves transnational copyright infringement as it concerns copyright in photographs²¹⁴ taken by an Austrian photographer which were later reproduced in Germany without the copyright holder's authorisation.

The case was referred to the European Court by the Handelsgericht Wien (Commercial Court, Vienna). The referring court asked questions of interpretation regarding jurisdiction for related actions in accordance with Article 6(1) of Brussels I. The other questions relate to Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the Information Society.

The applicant in the main proceedings is a freelance photographer. In the course of her work, she produced portrait photos of the Austrian national Natasha K²¹⁵ prior to her abduction in 1998. The five defendants²¹⁶ in the main proceedings are newspaper publishers. Only the first defendant in the main proceedings is established in Austria. The last four defendants are established in Germany. All five defendants published daily newspapers in Germany and most of them also published in Austria.

²¹² Case C-145/10 *Eva-Maria Painer v Standard VerlagsGmbH* [2012] ECDR 6.

²¹³ The Opinion of Advocate General Trstenjak was delivered on the 12 April 2011.

²¹⁴ Under Recital (16) and Article 6 of Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights [2006] OJ L372/12, photographs which are original in the sense that they are the author's own intellectual creation shall be protected.

²¹⁵ Natascha Maria Kampusch (now an Austrian television hostess) is known for her abduction at the age of 10 on 2 March 1998. She was held in a secret cellar by her kidnapper for more than eight years until she escaped on 23 August 2006.

²¹⁶ The five defendants are Standard VerlagsGmbH, Axel Springer AG, Süddeutsche Zeitung GmbH, Spiegel-Verlag Rudolf Augstein GmbH & Co KG and, lastly, Verlag M DuMont Schauberg Expedition der Kölnischen Zeitung GmbH & Co KG.

In 2006, Natasha K escaped from her abductor. The main proceedings concern the reporting by the defendants of this event using the applicant's photos but without crediting the applicant. Owing to the place of establishment of most of the defendants, many of the contested photos were published in Germany in newspapers and magazines such as *Der Standard*, *Süddeutsche Zeitung*, *Der Spiegel*, *Express*, *Bild*, and *Die Welt* (all of which run a news website on the internet). In some of the reports, a photo-fit was also published which was intended to show the presumed current appearance of Natasha K. It was produced by a graphic artist using a computer programme and based on one of the contested photos.

In the main proceedings, the applicant brought an action against the defendants at the *Handelsgericht Wien* in Austria. That action sought, in essence, a prohibitory injunction relating to the reproduction of the contested photos/photo-fit without her consent and without indicating her as author and payment of remuneration/damages.

As regards the PIL point referred by the Commercial Court, Vienna, the CJEU held that Article 6(1) of Brussels I must be interpreted as not precluding its application solely because actions against several defendants for substantially identical copyright infringements are brought on national legal grounds which vary according to the Member States concerned. The European Court stated that it is for the referring court to assess in the light of all the elements of the case, whether there is a risk of irreconcilable judgments if those actions were determined separately.

One of the intellectual property points referred by the Viennese court was whether a portrait photograph could be protected by copyright under Article 6 of Directive 2006/116/EC of the European Parliament and of the Council 12 December 2006 on the term of protection of copyright and certain related rights. The CJEU replied in the affirmative, so long as the photograph is an intellectual creation of the author reflecting his personality and expressing his free and creative choices in the production of that photograph.

3.6.3 *Peter Pinckney v KDG Mediatech AG*²¹⁷

This preliminary ruling concerned the interpretation of Article 5(3) of Brussels I in the context of alleged infringed copyright. The main proceedings commenced in the

²¹⁷ Case C-170/12 *Peter Pinckney v KDG Mediatech AG* [2013] ECDR 15.

Tribunal de grande instance de Toulouse (Regional Court, Toulouse) where the claimant sought compensation for damage sustained after the defendant allegedly reproduced 12 of the plaintiff's songs without his authorisation. The music works had been reproduced on compact discs which had been pressed in Austria by Mediatech and then marketed online by UK companies. The relevant websites were accessible from the claimant's residence in Toulouse.

Mediatech challenged the jurisdiction of the French courts. Ultimately the Cour d'appel de Toulouse held that the Tribunal de grande instance de Toulouse lacked jurisdiction on the ground that the defendant was domiciled in Austria and the place where the damage occurred could not be situated in France.

The claimant appealed that judgment, relying on Article 5(3) of Brussels I. He argued that the French courts have jurisdiction and that his action was wrongly rejected. In those circumstances, the Cour de Cassation decided to stay its proceedings and to refer two questions to the CJEU for a preliminary ruling.

1. Article 5(3) of ... [the Regulation] to be interpreted as meaning that, in the event of an alleged infringement of copyright committed ... online...
 -
 - the person who considers that his rights have been infringed has the option of bringing an action to establish liability before the courts of each Member State in the territory of which content placed online is or has been accessible, in order to obtain compensation solely in respect of the damage suffered on the territory of the Member State of the court before which the action is brought,
 - or
 - does that content also have to be, or to have been, directed at the public located in the territory of that Member State, or must some other clear connecting factor be present?
2. Is the answer to Question 1 the same if the alleged infringement of copyright results, not from the placing of dematerialised content online, but, as in the

present case, from the online sale of a material carrier medium which reproduces that content?²¹⁸

In its analysis of the referred questions, the CJEU referred to two of its fairly recent rulings concerning online torts which produced effects in numerous places. The first, joined cases *eDate Advertising GmbH v X; and Martinez v MGN Ltd*²¹⁹ concerned alleged infringement of personality rights on the internet while the second, *Wintersteiger*²²⁰ concerned alleged online infringement of trade marks in the context of Adwords in the advertising system on Google Internet.

The CJEU identified a number of principles arising from the two aforementioned rulings.

Firstly, the place where the alleged damage occurred within the meaning of Article 5(3) may vary according to the nature of the right allegedly infringed.²²¹ Secondly, the likelihood of the damage occurring in a particular Member State is subject to the requirement that the right in respect of which infringement is alleged is protected in that Member State.²²² Thirdly, in order to attribute jurisdiction to a court to hear an allegation of infringement in matters of tort, delict and quasi-delict, the identification of the place where the alleged damage occurred also depends on which court is best placed to determine whether the alleged infringement is well founded.²²³

In applying those principles for the purpose of localising the damage on the internet, the CJEU has distinguished between infringement of personality rights and infringement of intellectual and industrial property rights.²²⁴

²¹⁸ Ibid para H4.

²¹⁹ Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH v X; Olivier Martinez and Robert Martinez v MGN Ltd* [2011] ECR I-10269.

²²⁰ Case C-523/10 *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH* [2013] CEC 15.

²²¹ Case C-170/12 *Pinckney v KDG Mediatech* [2013] ECDR 15, para 32.

²²² Ibid para 33.

²²³ Ibid para 34.

²²⁴ Ibid para 35.

Where there is an infringement of personality rights (which are protected in all the Member States) by way of content placed online, the victim of such infringement may bring his action before the courts of each Member State in the territory of which content placed online is or has been accessible.²²⁵ However, such courts' jurisdiction is delimited to the damage caused in the territory of the Member State of the court seised.²²⁶ Staying with the theme of injury to personality rights by content placed online, the CJEU suggested that such a case might best be assessed by the court of the place where the alleged victim has his centre of interests. Moreover, the alleged victim may choose to bring an action in one forum in respect of all the damage caused.²²⁷

As regards the second part of the question referred by the Cour de Cassation, pertaining to the possible directing at the public of online infringing content, the court stated that the localisation of the place where the harmful event giving rise to that damage occurred, for the purposes of Article 5(3) Brussels I, cannot depend on criteria which are specific to the examination of the substance and which do not appear in that provision.²²⁸ As the sole condition specified in Article 5(3) is that a harmful event has occurred or may occur, there is no requirement that the activity be 'directed' to the Member State in which the court seised is situated.²²⁹ In that regard, Article 5(3) differs from Article 15(1)(c) of Brussels I, which was interpreted in Joined Cases C-585/08 and C-144/09 *Pammer; and Hotel Alpenhof*.²³⁰

In terms of jurisdiction to hear an action in tort, delict or quasi-delict, that will already be established in favour of the court seised if the Member State in which the court is situated protects the copyrights relied on by the plaintiff and there is a likelihood that the alleged harmful event might occur within the jurisdiction of the court seised.²³¹ That

²²⁵ Ibid para 36.

²²⁶ Ibid para 36; Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH v X; Olivier Martinez and Robert Martinez v MGN Ltd* [2011] ECR I-10269, para 52.

²²⁷ Case C-170/12 *Pinckney v KDG Mediatech* [2013] ECDR 15, para 36.

²²⁸ Ibid para 41.

²²⁹ Ibid paras 41 and 42.

²³⁰ Joined Cases C-585/08 and C-144/09 *Pammer v Reederei Karl Schlüter; Hotel Alpenhof v Oliver Heller* [2010] ECR I-12527; see para 2.10.

²³¹ Case C-170/12 *Pinckney v KDG Mediatech* [2013] ECDR 15, para 43.

likelihood arises from the possibility of obtaining a reproduction of the protected work from an internet site accessible within the jurisdiction of the court seised.²³²

The CJEU then seemed to delimit the jurisdiction of the court seised. It stated that if the protection granted by the Member State of the seised court is applicable only in that Member State, then that court only has jurisdiction to determine the damage caused within the Member State in which it is situated.²³³ The first part of this statement seems somewhat tautologous as copyright protection will be, by its nature, territorial in nature. Copyright protection provided by a specific EU Member State will be ‘confined’ to the territory of that country. It cannot extend beyond the borders of that particular State. The rationale for this delimitation of jurisdiction (as to damage) is to ensure that the seised court cannot substitute itself for foreign courts particularly when the damage has occurred abroad and said courts are best placed to ascertain whether the copyrights protected by the Member State concerned have been infringed, and the nature of the harm caused.²³⁴

This thesis argues that *Pinckney* fails to address the requirement in *Dumez*²³⁵ and *Marinari*²³⁶ for damage under Article 5(3) of Brussels I to be direct before a court may assume jurisdiction. On the facts of *Pinckney*, there is a strong case for arguing that the damage alleged in France was indirect in nature as the illegal CDs were pressed in Austria (infringing, if anything, the Austrian reproduction right) and then later marketed online by UK companies. Any online sales that would ensue would infringe the claimant’s distribution rights (under Article 4, InfoSoc Directive)²³⁷ in the UK and, arguably, in every country to which the illicit CDs are sent. Given that the principal damage was occurring outside France, indirect damage was all that could really occur within France.

²³² Ibid para 44.

²³³ Ibid para 45.

²³⁴ Ibid para 46.

²³⁵ Case C-220/88 *Dumez France SA v Hessische Landesbank* [1990] ECR I-49; see para 4.2.2.

²³⁶ Case C-364/93 *Marinari v Lloyds Bank plc* [1995] ECR I-2719; see para 4.2.3.

²³⁷ Article 4(1) of Directive 2001/29/EC provides that Member States shall provide for authors, in respect of the original of their works or of copies thereof, the exclusive right to authorise or prohibit any form of distribution to the public by sale or otherwise.

3.6.4 *Football Dataco Ltd v Sportradar*²³⁸

While admittedly, *Football Dataco* does not concern digital copyright, it does concern digital databases and digitised data. The relevant legal instrument, Directive 96/9/EC (the Directive on the legal protection of databases) introduced two forms of protection for databases - the *sui generis* database right and database copyright, but they are closely linked. Despite being independent of each other, the two protections may subsist in respect of the same database. While acknowledging the structure/contents dichotomy²³⁹ in terms of databases, one also has to acknowledge the proximity that exists between the two distinct but related IPRs of the database right and copyright.

The relevance of *Football Dataco* to this thesis derives from a number of factors. Firstly, the ruling contains analysis of two key tort PIL provisions, namely, Article 5(3), Brussels I and Article 8(1), Rome II. Secondly, the merits and demerits of two classic communication theories are well ventilated in the ruling. Thirdly, the issue of localising an act of re-utilisation on the internet is discussed and, lastly, the condition of targeting persons in a particular territory (analogous to a trader directing its activity to the Member State of the consumer's domicile, as per joined cases *Peter Pammer; and Hotel Alpenhof*)²⁴⁰ is laid down by the court in the context of localising an unauthorised act of re-utilisation.

3.6.4.1 *The dispute in the main proceedings*

Football Dataco and others are responsible for organising football competitions in England and Scotland. Football Dataco Ltd manages the creation and exploitation of the data and intellectual property rights relating to those competitions. Football Dataco and Others claim to have, under UK law, a *sui generis* right in the 'Football Live' database.

²³⁸ Case C-173/11 *Football Dataco Ltd v Sportradar* [2013] CMLR 29.

²³⁹ The *sui generis* database right protects the investment employed in obtaining, verifying and presenting the contents of a database. Database copyright protects the intellectual creation involved in the selection and arrangement of the data within the database, i.e. the structure of the database and not the individual contents (although they may be the subject of separate copyright protection). See: David Rose and Nina O' Sullivan, 'Football Dataco v Yahoo! Implications of the ECJ judgment' (2012) 7 *Journal of Intellectual Property Law & Practice* 792, 793.

²⁴⁰ See para 2.10.

Football Live is a compilation of data about football matches in progress collected mainly by ex-professional footballers who work for Football Dataco. Football Dataco submits that the obtaining and/or verification of the data requires substantial investment and that the compilation of the database involves considerable skill, effort, discretion and/or intellectual input.

Sportradar GmbH, a German company, provides results and other statistics relating inter alia to English league matches live via the internet. Its service is called 'Sport Live Data' and it operates a website called betradar.com. Betting companies which are customers of Sportradar GmbH entered into contracts with the Swiss holding company Sportradar AG, which is the parent company of Sportradar GmbH. Some of the customers are companies incorporated under UK law (e.g. bet365) and Gibraltar law (e.g. Stan James) which provide betting services aimed at the UK market. The customers' websites contained a link to Sportradar's website. When internet users clicked on the 'Live Score' option, the data appeared under a reference to 'bet365' or 'Stan James'. The referring court concluded that members of the public in the UK clearly formed an important target for Sportradar.

In April 2010, Football Dataco and Others brought proceedings against Sportradar in the English High Court (Chancery Division) seeking compensation for damage linked to an infringement by Sportradar of their *sui generis* right. In July 2010, Sportradar challenged the jurisdiction of the High Court to hear the case. Later that month Sportradar GmbH brought proceedings against Football Dataco in the Landgericht Gera (Regional Court, Gera) Germany, seeking a negative declaration that its activities did not infringe any IPRs held by Football Dataco.

In November 2010, the High Court declared that it had jurisdiction to hear the action brought by Football Dataco in so far as it concerned the joint liability of Sportradar and its customers using its website in the UK for infringement of their *sui generis* right by acts of extraction and or re-utilisation. By contrast, it declined jurisdiction over the action brought by Football Dataco in so far as it concerned the primary liability of Sportradar for such an infringement.

Both, Football Dataco and Sportradar, appealed against that judgment to the English Court of Appeal (Civil Division). The Court of Appeal decided to stay the proceedings and to refer the following question to the CJEU for a preliminary ruling.

Where a party uploads data from a database protected by the *sui generis* right under Directive 96/9/EC ...onto that party's web server located in Member A and in response to requests from a user in another Member State B the web server sends such data to the user's computer so that the data is stored in the memory of that computer and displayed on its screen:

- 1) Is the act of sending the data an act of 'extraction' or 're-utilisation' by that party?
- 2) Does any act of extraction and/or re-utilisation by that party occur
 - a) In A only?
 - b) In B only; or
 - c) In both A and B?²⁴¹

3.6.4.2 The Territoriality of the Sui Generis Right

As regards the protection provided by the *sui generis* right, the CJEU circumscribed this by stating that it is 'limited in principle' to the territory of the Member State in which it is situated so that the person enjoying its protection can only rely on it against unauthorised acts of re-utilisation which take place in that territory.

The CJEU noted that the referring court had to assess the validity of the claims of Football Dataco alleging infringement of the *sui generis* right they claim to hold, under UK law, in the Football Live database. For that assessment, it would be necessary to know whether the acts of sending data at issue fall, as acts taking place within the UK, within the territorial scope of the protection by the *sui generis* right afforded by the law of that Member State.

The European Court then proceeded to set out the EU PIL provisions relevant to the case. Given the tortious nature of the alleged unauthorised acts of re-utilisation, the CJEU identified the special jurisdiction rule - Article 5(3) of Regulation 44/2001 - as

²⁴¹ Case C-173/11 *Football Dataco v Sportradar GmbH* [2013] CMLR 29, para 17.

the relevant jurisdictional rule.²⁴² The CJEU believed that the issue of localising the acts of sending the data would influence the question of the jurisdiction of the referring court, particularly as regards the action seeking to establish the principal liability of Sportradar in the dispute before that court.²⁴³

In terms of the applicable law, the CJEU identified Article 8(1) of Regulation 864/2007 (Rome II) as the relevant rule. It relates to IPRs that cannot be classified as *unitary* Community rights and states that the applicable law in cases of IPR infringement will be ‘the law of the country for which protection is claimed’.²⁴⁴ In essence, this PIL rule confirms the importance of ascertaining whether the infringing acts in the main proceedings took place in the UK, the country where Football Dataco claims protection for the Football Live database, by way of the *sui generis* right.²⁴⁵

3.6.4.3 Re-utilisation by means of a web server

Referring to the Advocate-General’s Opinion, the court remarked that re-utilisation carried out by a web server is characterised by a series of successive operations, ranging at least from the placing online of the data concerned on that website for it to be consulted by the public to the transmission of that data to the interested members of the public, which may take place in the territory of different Member States.²⁴⁶ However, the court was at pains to distinguish this method of making available to the public from traditional modes of distribution. Unlike traditional modes of distribution, a website can be consulted instantly by an unlimited number of internet users throughout the world irrespective of any intention on the part of the operator of the website.²⁴⁷

The court concluded that the mere fact that the website containing the data in question is accessible in a particular national territory is not a sufficient basis for concluding that the operator of the website is performing an act of re-utilisation caught by the national law applicable in that territory.²⁴⁸ In other words, the fact that data on Sportradar’s

²⁴² Ibid para 29.

²⁴³ Ibid para 30.

²⁴⁴ Ibid para 31.

²⁴⁵ Ibid para 32.

²⁴⁶ Ibid para 34.

²⁴⁷ Ibid para 35.

²⁴⁸ Ibid para 36.

server is sent to an internet user's computer in the UK is not in itself a sufficient basis for concluding that the act of re-utilisation performed by Sportradar takes place in the territory of the UK.²⁴⁹

3.6.4.4 Evidence of an intention to target persons in a different Member State

Rather, for an act of re-utilisation to be localised in the territory of the Member State to which the data is sent, there must be evidence that the act discloses an intention on the part of its performer to target persons in that territory.²⁵⁰

The CJEU then offered as examples, elements or circumstances within the main proceedings which might constitute evidence of the performer's intention to target persons in the UK. They include the following facts: 1. The data on Sportradar's server related to English football matches;²⁵¹ 2. Sportradar granted by contract the right of access to its servers to companies offering betting services to the UK public, if Sportradar were aware (or must have been aware) of the specific destination of services;²⁵² 3. The data placed online by Sportradar is accessible to UK internet users (who are customers of the betting companies) in their own language, which differs naturally from the languages used in Germany and Switzerland - the States from which Sportradar pursues its activities.²⁵³

The court held that where such evidence is present, the referring court would be entitled to consider that an act of re-utilisation such as that in the main proceedings is located in the Member State of location of the user *to whose* computer the data in question is transmitted for the purpose of storage and display on screen (Member State B).²⁵⁴ It rejected Sportradar's argument that an act of re-utilisation must in all circumstances be

²⁴⁹ Ibid para 38.

²⁵⁰ Ibid para 39. By analogy, the court alluded to: Joined Cases C-585/08 and C-144/09 *Pammer v Reederei Karl Schlüter; Hotel Alpenhof v Oliver Heller* [2010] ECR I-12527, paras 75, 76, 80 and 92; Case C-324/09 *L'Oreal SA and Others v eBay International AG and Others* [2011] ECR I-6011, para 65; and Case C-5/11 *Criminal proceedings against Titus Alexander Jochen Donner* (CJEU (Fourth Chamber), 21 June 2012) paras 27 et seqq.

²⁵¹ Case C-173/11 *Football Dataco v Sportradar GmbH* [2013] CMLR 29, para 40.

²⁵² Ibid para 41.

²⁵³ Ibid para 42.

²⁵⁴ Ibid para 43.

regarded as located exclusively in the Member State in which the web server from which the data in question is sent is situated.²⁵⁵ By doing so, the court also implicitly rejected application of the emission theory.

3.6.4.5 Rejection of the Emission Theory²⁵⁶

The court then went on to give a number of reasons for its rejection of the emission theory. It referred to the frequent difficulties experienced in localising the originating server and the risks inherent in applying the emission theory if the infringer's server is located outside the territory of the State whose public is targeted.²⁵⁷ The application of the emission theory might also undermine the effectiveness of the protection offered to the database, based as it is on the national law of the country where the database is located. Moreover, the protection of databases would, in general, be compromised, if acts of re-utilisation aimed at the public in the EU were deemed to be outside the scope of Directive 96/9 because the server of the website used by the infringer was located in a third country.²⁵⁸

In a somewhat ambiguous ruling, the CJEU confirmed that the unauthorised re-utilisation took place in 'at least' Member State B (the State of receipt) so long as there is evidence that the act disclosed an intention on the part of the sender of the data to target members of the public in that State (and this factor must be assessed by the national court). By using the term 'at least', the court leaves the door open for a finding of localisation in both the State of transmission and the State of receipt. This thesis asserts that this lack of certainty assists potential infringers of the database right. They can still exploit the relative vagueness of the CJEU's ruling and migrate their servers either to a third country or to an EU Member State whose courts or legal framework might favour them. From there, they could still carry out illegal re-utilisations in the hope (ultimately) that the act of re-utilisation be localised in the country of emission and that any decision as to jurisdiction would follow and be conferred on the courts of the country of emission.

²⁵⁵ Ibid para 44.

²⁵⁶ The Emission Theory is discussed at para 3.6.4.5.

²⁵⁷ Ibid para 45.

²⁵⁸ Ibid para 46.

In failing to answer the question posed by the referring court as to whether the act of re-utilisation occurred in *both* State A and State B, the Court of Justice did not go as far as Advocate General Cruz Villalón who, four months earlier, did not choose one of the two traditional communication theories over the other. Instead, he opined that the act of re-utilisation took place in *both* Member State A and Member State B.²⁵⁹

3.6.4.6 Communication Theory or Emission Theory?

Another way of looking at the CJEU ruling is that it favours the communication theory²⁶⁰ over the emission theory, but without fully dismissing the latter either! Intriguingly, the court also stipulates the ‘add-on’ of evidence of the sender’s intention to target members of the public in the State of receipt. In this regard, the court does follow Advocate General Cruz Villalón who describes the ‘idea of the intended target of information on the internet’ as a ‘suitable criterion’.²⁶¹ Importantly, the notion of intentional targeting does not seem to jar with the definition of ‘re-utilisation’ under Article 7(2)(b) of Directive 96/9 which refers to ‘any form of making available to the public the content of a protected database.’ It is interesting to note too that this case applies the condition of targeting members of the public in a specific country, to the database right. . Previously, the senior EU court had applied this particular condition to the areas of e-commerce (*Pammer; and Hotel Alpenhof*), the offer for sale of goods through the use of an unauthorised trade mark (*L’Oreal*²⁶²) and, the directing of advertising at members of the public (*Donner*²⁶³). While it may still be a bit too early to pass judgment on this development, it does not seem an illogical evolution and there is the IP precedent of *L’Oreal*.

3.7 Conclusions

In this chapter, I have painted a scenario where the three principal elements of this PhD feature prominently. Inevitable links arise as between the internet (and ICT more

²⁵⁹ Case C-173/11 *Football Dataco v Sportradar GmbH* Opinion of AG Cruz Villalón (21 June 2012), paras 60 et seq.

²⁶⁰ See para 6.13.

²⁶¹ *Ibid* para 56.

²⁶² Case C-324/09 *L’Oreal SA and Others v eBay International AG and Others* [2011] ECR I-6011.

²⁶³ Case C-5/11 *Criminal proceedings against Titus Alexander Jochen Donner* (CJEU (Fourth Chamber), 21 June 2012).

broadly), copyright and PIL. Given that both the internet and satellite communication frequently involve a transborder element, PIL issues will arise where copyright infringing material is disseminated over such media. When one factors in high levels of transborder copyright infringement, then it becomes clear that PIL rules will be invoked more and more in the Digital Age.

Lucasfilm is a good example of a case concerning transborder copyright issues which involved judicial interpretation of justiciability issues. The outcome was somewhat surprising as the UK Supreme Court held it did have jurisdiction over a copyright infringement which occurred abroad, *so long as it could establish in personam* jurisdiction over the defendant. This seems to contradict Section 16(1), CDPA 1988 (concerning territoriality) which stipulates that for UK Copyright Law to apply, the infringing acts must take place in the UK. The Supreme Court also emphasised the fact that the modern trend was in favour of the enforcement of foreign IPRs.

During the analysis of the rulings in this chapter, it became evident that highly relevant sub-themes featured prominently. They include: justiciability and *in personam* jurisdiction (*Lucasfilm*), the complex interface between IPRs and IT (e.g. the instance of encrypted audiovisual content in the *Football Association Premier League* preliminary ruling), the ease with which infringing activities can assume a transnational character particularly where a common language is at play (e.g. Germany and Austria, in *Eva-Maria Painer* (Advocate-General's Opinion)) and, lastly, the notion of targeting persons in a foreign country, as applied in the discrete fields of e-commerce, localisation of the act of re-utilisation (database right) (*Football Dataco Ltd*), and localisation of the communication to the public right in copyright.

There seem to be interesting parallels between the *Pinckney* ruling and the holding in *Fiona Shevill v Presse Alliance*.²⁶⁴ In *Pinckney*, the CJEU limited the jurisdiction of courts situated in the territory where an infringement of personality rights occurred. Following on from the *eDate Advertising and Martinez* ruling, referred to in *Pinckney*, each court only has jurisdiction in respect of damage caused in the country where it is

²⁶⁴ Case C-68/93 *Fiona Shevill, Ixora Trading Inc, Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-415. The *Shevill* case is discussed at 4.2.3.3.

situated.²⁶⁵ In a passage of *Pinckney* ruling that is somewhat unclear, the CJEU seems to suggest that the courts of the place where the alleged victim has his centre of interests may be permitted to adjudicate in respect of all of the damage caused.²⁶⁶ In *Shevill*, a case concerning alleged libel, the ECJ ruled that the courts of the place where the publisher of the defamatory publication is established have jurisdiction to award damages for *all* the harm caused by the defamation (analogous to courts of the place of the victim's centre of interests) while the courts of each of the Member States in which the publication was distributed (and where the victim suffered injury to reputation) would only have jurisdiction to rule in respect of harm caused in their particular Member State (analogous to the situation spelt out in *eDate Advertising and Martinez* above).²⁶⁷

The issue of the localisation of the re-utilisation act is prominent in *Football Dataco*. It seems that the CJEU came down in favour of the communication theory in contrast with Advocate-General Villalón who regarded the communication theory and the emission theory as being of equal importance. However, the court stipulated that for the communications theory to apply, there must also be evidence of an intention to target persons in the foreign country. This is interesting in that a similar requirement of targeting was laid down by the English High Court in the context of the localisation of the communication to the public right in online contexts. The requirement was set out by Arnold J in a number of the web-blocking cases which are treated more fully in chapter 7, from para 7.3.5. on.

²⁶⁵ Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH v X; Olivier Martinez and Robert Martinez v MGN Ltd* [2011] ECR I-10269, para 52.

²⁶⁶ Case C-170/12 *Peter Pinckney v KDG Mediatech AG* [2013] ECDR 15, para 36.

²⁶⁷ Case C-68/93 *Fiona Shevill, Ixora Trading Inc, Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-415, Operative part 1.

Chapter 4. Private International Law – Jurisdiction

TABLE OF CONTENTS

4.1 Introduction	101
4.2 Jurisdiction.....	101
4.2.1 The basic rule of jurisdiction.....	105
4.2.2 Special jurisdictional provisions.....	107
4.2.2.1 Article 5 (3) of Brussels I.....	108
4.2.3 Important case law relating to Article 5 (3).....	110
4.2.3.1 The definition of the term ‘tort’ under the Brussels regime	110
4.2.3.2 <i>Handelskwekerij G J Bier v Mines de Potasse d’Alsace</i> (the Reinwater case).....	111
4.2.3.3 Transnational torts and the extent of jurisdiction of courts	115
4.2.3.4 Indirect economic loss cannot found jurisdiction	119
4.2.4 The new Article 5 (3)	122
4.2.5 How will the new Article 5 (3) operate in practice?	124
4.2.6 Lis Pendens.....	125
4.2.6.1 Provisional Measures	127
4.3 Conclusions.....	128

*'Conflict of laws is regarded as an arcane science far removed from real world concerns, and characterized by an esoteric vocabulary, it inevitably attracts speculative minds whose forte is not necessarily common sense.'*²⁶⁸

4.1 Introduction

In many ways, this thesis constitutes a 'laboratory' in which the EU tort PIL rules will be examined for efficacy in an online environment. Given the natural demarcation between jurisdictional issues and applicable law issues, I have decided to treat these two main PIL components separately. Therefore, this chapter will be devoted to a 'survey' of jurisdictional issues while chapter 5 will be devoted to a 'survey' of applicable law issues.

The objective of this chapter is to analyse and evaluate the EU jurisdictional framework with the Brussels I Regulation constituting the main focus. The core of this chapter is, in fact, an analysis of Articles 2 and 5(3), Brussels I. The former is the fundamental rule of the general jurisdictional framework while the latter is a special jurisdiction provision concerning torts, delicts and quasi-delicts. The chapter also covers important case law generated under the old Brussels Convention 1968, an analysis of the *lis pendens* provisions of Brussels I (Articles 27-30) and the provisional measures provision of Brussels I (Article 31).

4.2 Jurisdiction

This section will have as its principal focus the Brussels I Regulation which came into force on 1 March 2002 and now applies either directly or indirectly²⁶⁹ in all 28 EU

²⁶⁸ Friedrich K Juenger, *Selected Essays on the Conflict of Laws (Transnational Classics in International Law, 1)* (1st edn, Transnational Pub 2000) ix (emphasis added).

²⁶⁹ The provisions of the Brussels I Regulation with minor modifications are applied by international law to the relations between the EU and Denmark. This is achieved by way of the Agreement between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2005] OJ L299/62.

Member States. This instrument harmonises to a large extent the jurisdictional rules for civil and commercial matters²⁷⁰ within the EU.

Brussels I

Council Regulation (EC) 44/2001 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters, also known as Brussels I, the Brussels Regulation or the Judgments Regulation,²⁷¹ was adopted by the EU Council of Ministers on 22 December 2000.²⁷² On 1 March 2002, Brussels I entered into force²⁷³ when it superseded the Brussels Convention 1968.²⁷⁴ The Regulation is directly applicable in all 28 EU Member States with the exception of Denmark. However, under the EU/Denmark Agreement, the provisions of the Regulation, with minor modifications

²⁷⁰ Brussels I does not cover revenue, customs or administrative matters (Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1, art 1(1)).

²⁷¹ The Brussels Regulation 44/2001 is referred to as the Judgments Regulation in David McClean and Veronica Ruiz Abou-Nigm, *Morris - The Conflict of Laws* (8th edn, Sweet & Maxwell 2012).

²⁷² Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1. Bénédicte Fauvarque-Cosson, 'Comparative Law and Conflict of Laws: Allies or Enemies? New Perspectives on an Old Couple' (2001) 49 AJCL 407, 418 refers to the 'communitarization of conflicts law under the Treaty of Amsterdam'. (This expression was coined by Jürgen Basedow, 'The communitarization of the conflict of laws under the Treaty of Amsterdam' (2000) 37 CMLR 687.) Articles 61 and 65 of the Amsterdam Treaty greatly increased the Community's powers in the field of conflict of laws.

²⁷³ Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1, art 76. Interestingly, the EU chose to achieve its aims by way of Regulation rather than Directive. In doing so, the EU ensured that the provisions of the Regulation would be binding and directly applicable from the date upon which the Regulation entered into force i.e. 1 March 2002.

²⁷⁴ *Ibid* art 68.

are applied by international law to the relations between the Union and Denmark.²⁷⁵ On 1 January 2010, the new Lugano Convention came into force between the EU Member States (including Denmark) and Norway. This new convention reflects the changes made by the Brussels I Regulation to the Brussels Convention. As a consequence, the old Lugano Convention also had to be revised so as to reflect the changes.

Described by one commentator as 'the basic jurisdictional statute for the Member States',²⁷⁶ Brussels I covers jurisdiction and enforcement of judgments in civil and commercial matters.²⁷⁷ While Brussels I sets out general jurisdiction rules, it should be noted that certain EU IP legal instruments contain specific jurisdiction provisions. They

²⁷⁵ Agreement between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2005] OJ L299/62, art 2(1). For consequential amendments in the UK see The Civil Jurisdiction and Judgments Regulations 2007, SI 2007/1655. The Agreement applies to legal proceedings instituted after its entry into force (on 1 July 2007) in Article 9(1) of the Agreement. There is a separate EU/Denmark Agreement, the Agreement between the European Community and the Kingdom of Denmark on the service of judicial and extrajudicial documents in civil or commercial matters [2008] OJ L331/21, which extends the terms of the Regulation (EC) 1393/2007 of the European Parliament and of the Council of 13 November 2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents), and repealing Council Regulation (EC) 1348/2000 [2007] OJ L324/79, in short referred to as the Service Regulation, to Denmark.

²⁷⁶ Adrian Briggs, *The Conflict of Laws* (2nd edn, OUP 2008) 58. Morrison and Gillies point out that while Brussels I harmonises jurisdictional rules in civil matters within the EU, it will have absolutely no effect on copyright issues or jurisdiction in copyright disputes originating outside the EU. Alex Morrison and Lorna E Gillies, 'Securing Webcast Content in the European Union: Copyright, Technical Protection and Problems of Jurisdiction on the Internet' (2002) 24 EIPR 74, 80.

²⁷⁷ Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1, Recital (7) circumscribes the scope of the Regulation. It provides as follows: 'The scope of this Regulation must cover all the main civil and commercial matters apart from certain well-defined matters.' The scope of the Regulation is governed by Article 1 which provides as follows: 'This Regulation shall apply in civil and commercial matters whatever the nature of the court or tribunal. It shall not extend, in particular, to revenue, customs or administrative matters.'

are the Community Trade Mark Regulation,²⁷⁸ the Community Design Regulation²⁷⁹ and the Community Plant Variety Regulation.²⁸⁰ Each contains a particular jurisdiction provision for infringement and invalidity proceedings. Similarly, the European Patent Convention has a Jurisdiction Protocol where there is a dispute as to the entitlement of a European patent. This Protocol confers jurisdiction on particular contracting states in accordance with a set of jurisdiction rules.

Following the establishment of Community competence in the field of PIL, by way of the Treaty of Amsterdam, Brussels I became one of a number of measures adopted by the Community so as to progressively establish an area of freedom, security and justice within the Community. These measures relate to judicial co-operation in civil matters which is necessary for the sound operation of the internal market.²⁸¹ Acknowledging that differences between national rules governing jurisdiction and recognition of judgments hamper the sound operation of the internal market, Brussels I was adopted to unify the rules of conflict of jurisdiction in civil and commercial matters and to simplify the formalities with a view to rapid and simple recognition and enforcement of judgments from Brussels I Member States.²⁸²

²⁷⁸ Council Regulation (EC) 40/94 of 20 December 1994 on the Community trade mark [1994] OJ L11/1, art 93 ('International Jurisdiction' provision).

²⁷⁹ Council Regulation (EC) 6/2002 of 12 December 2001 on Community designs [2002] OJ L3/1, art 82 ('International Jurisdiction' provision).

²⁸⁰ Council Regulation (EC) 2100/94 of 27 July 1994 on Community plant variety rights [1994] OJ L 227/1, art 101 ('Jurisdiction and Procedure in Legal Actions Relating to Civil Law Claims'). Article 101(3) provides that proceedings relating to actions in respect of claims for infringement may also be brought in the courts for the place where the harmful event occurred. In such cases, the courts shall have jurisdiction only in respect of infringements alleged to have been committed in the territory of the Member State to which it belongs.

²⁸¹ Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1, Recital (1).

²⁸² Ibid Recital (2).

4.2.1 *The basic rule of jurisdiction*

The basic rule of jurisdiction based on the defendant's domicile continues to apply in Brussels I.²⁸³ It is contained in Article 2(1) of the Regulation and provides as follows:

'Subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State.'²⁸⁴

The Regulation adopts the principle that, in general, persons should be sued in the courts of the Regulation State where they are domiciled.²⁸⁵ The words 'shall (...) be

²⁸³ Adrian Briggs, *The Conflict of Laws* (2nd edn, OUP 2008) 59 where he states: 'as the basic principle is that a defendant shall be sued in the courts of the Member State where he is domiciled, a provision of the Regulation derogating from this rule will tend to receive a restrictive construction.'

²⁸⁴ From an Internet perspective, this provision makes a lot of sense since frequently, in online copyright infringement scenarios, the infringer (defendant) has infringed intellectual property rights in a number of different jurisdictions. By stipulating that the defendant be sued in the courts of the Contracting State where he is domiciled, Article 2 centralises the proceedings in one State even though the defendant's actions may have negatively affected the plaintiff copyright-holder's interests in a number of different States. However, given the ease with which safe haven relocation can occur in an Internet context, perhaps a new jurisdiction rule enabling the plaintiff to sue in his country of domicile for the global infringement of his rights is now required. Admittedly, such a rule would represent a radical departure from existing PIL principles. Torremans suggests that the plaintiff should be allowed to rely upon this rule only if he can demonstrate to the court that it is not feasible to sue the defendant in his domicile due to the lack in that domicile of intellectual property laws that meet the minimum public international law standard that has been established by the TRIPs Agreement. Paul Torremans, 'Private International Law Aspects of IP – Internet Disputes' in Lilian Edwards and Charlotte Waelde (eds) *Law and the Internet: a Framework for Electronic Commerce* (2nd edn, Hart Publishing 2000) 235.

²⁸⁵ Paul Jenard, Report on the Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters [1979] OJ C59/1, 13, 18 et seq. The following is stated at p 19 of the Report:

Defendants are usually sued in the courts of the State in which they are domiciled. This is true of proceedings in which there is no international element. It is also true of proceedings with an international element in which, by application of the traditionally accepted maxim '*actor sequitur forum rei*', the defendant is sued in the courts of the State of his domicile. The Convention does not therefore involve a

sued' should not be taken literally. Other bases of jurisdiction make it clear that the defendant may, and, in some circumstances, must, be sued in the courts of a Member State other than that of his domicile.²⁸⁶ Following *Owusu v Jackson*,²⁸⁷ Article 2 will apply where both the claimant and defendant are domiciled in the same Member State but the dispute between them is connected with a non-Member State, rather than with another Member State.

In fact, many of the Regulation's provisions turn on whether the defendant is domiciled in one of the EU Member States.²⁸⁸ The definition of domicile is not uniform.²⁸⁹ It is necessary to distinguish natural persons from companies or other legal persons or associations of persons, and from trusts.

Where the defendant is a natural person, reference must be made to Article 59 of the Regulation and paragraph 9 of Schedule 1 to the Civil Jurisdiction and Judgments Order 2001. Where the defendant is a legal person, reference should be made to Article 60 of the Regulation. Where the Member State in which the defendant is domiciled is the UK, the Modified Regulation will apply to allocate jurisdiction between the courts of England, Scotland and Northern Ireland.

general reversal of national rules of jurisdiction nor of the practice of judges and lawyers.

²⁸⁶ James Fawcett, Janeen Carruthers and Peter North, *Cheshire, North & Fawcett: Private International Law* (14th edn, OUP 2008) 227. It should be noted that where Article 27 (*lis pendens*) applies, it requires the court of Member States, including that of the defendant's domicile, to decline jurisdiction.

²⁸⁷ Case C-281/02 *Owusu v Jackson* [2005] ECR I-1383, paras 24-37.

²⁸⁸ Adrian Briggs, *The Conflict of Laws* (2nd edn, OUP 2008) 63.

²⁸⁹ Briggs states as follows:

There has been pressure to provide a single autonomous definition of domicile, or to abandon it *holus bolus* and move instead to the concept of habitual residence, not least because of variation in the separate national law definitions of domicile. But in the absence of a public register of status, however defined, it is difficult to see that such a change would accomplish very much of value.

Ibid 64.

4.2.2 *Special jurisdictional provisions*

Section 2 of Chapter II of Brussels I affords supplementary grounds of jurisdiction. Section 2 comprises Articles 5-7. They are referred to as special jurisdiction provisions since they enable jurisdiction to be granted to courts other than the courts of the Member State where the defendant is domiciled.²⁹⁰ This work will focus on Article 5 since it is of most relevance to this thesis. These special jurisdiction provisions may be chosen at the plaintiff's option. The plaintiff can only rely on Article 5 if the defendant is domiciled in one of the EU Member States.²⁹¹ The rationale behind the special jurisdiction provisions was set out in *Dumez France SA and Tracoba SARL v Hessische Landesbank*²⁹² where it was stated that special jurisdiction is

based on the existence of a particularly close connecting factor between the dispute and courts other than those of the State of the defendant's domicile, which justifies the attribution of jurisdiction to those courts for reasons relating to the sound administration of justice and the efficacious conduct of proceedings.²⁹³

Article 5 provides that a person domiciled in a Member State may be sued in another Member State in seven specified situations.²⁹⁴ The phrase 'may (in another Member

²⁹⁰ Tactical considerations also play a part in the plaintiff's decision about where to sue. These tactical considerations may have little to do with the subject matter of the conflict of laws. For example, judges in one possible forum (the place where suit is brought) may be likely to be more sympathetic to the plaintiff's contentions than judges in another place where suit can be brought. Russell J Weintraub, *Commentary on the Conflict of Laws* (4th edn, Foundation Press 2001) 2.

²⁹¹ This particular rule has not been changed by the revised Brussels I Regulation (Regulation 1215/2012), see fn 3.

²⁹² Case C-220/88 *Dumez France SA and Tracoba SARL v Hessische Landesbank* [1990] ECR I-49.

²⁹³ *Ibid* paras 79 et seq.

²⁹⁴ The seven situations are as follows: 1. Matters relating to contract; 2. Matters relating to maintenance; 3. Matters relating to tort, delict or quasi-delict; 4. In a civil claim for damages or restitution based on an act giving rise to criminal proceedings; 5. A dispute arising out of the operations of a branch, agency or other establishment; 6. In matters relating to a trust;

State) be sued' is not intended to confer on courts a discretion to refuse to take jurisdiction. Instead, it means that the plaintiff is permitted, but not required, to sue the defendant in a Member State other than that in which the defendant is domiciled. In essence, where Article 5 applies, the plaintiff is given a choice of fora. He can sue, by virtue of Article 2, in the Member State where the defendant is domiciled or in some other Member State or States, by virtue of Articles 5.²⁹⁵

4.2.2.1 Article 5(3) of Brussels I

Of the special jurisdiction provisions, Article 5(3) is the one of most relevance to this thesis. It is also of particular importance to IP lawyers. The wording of Article 5(3) is:

'A person domiciled in a Member State may, in another Member State, be sued, in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur'.

Article 5(3) entitles the claimant to sue the defendant in a Member State other than where the defendant is domiciled. Nonetheless, the defendant's domicile is the normal place for the trial and Article 5 is an exception to this general rule.²⁹⁶ Its provisions must not be given an interpretation going beyond the situations envisaged by the Regulation.²⁹⁷

Since infringement of an intellectual property right is characterised as tortious in common law jurisdictions²⁹⁸ and as delictual in civil law systems,²⁹⁹ it falls, accordingly,

7. In disputes concerning the payment of remuneration claimed in respect of the salvage of a cargo or freight.

²⁹⁵ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 32.

²⁹⁶ Case 56/79 *Zelger v Salinitri* [1980] ECR 89.

²⁹⁷ Case C-167/00 *Verein für Konsumenteninformation v Karl Heinz Henkel* [2002] ECR I-8111, Opinion of AG Jacobs, para 33.

²⁹⁸ *House of Spring Gardens Ltd v Waite* [1991] 1 QB 241 [253] (copyright); *Mölnlycke AB v Procter & Gamble Ltd* [1992] 1 WLR 1112, 1117 (patents); James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 151.

²⁹⁹ LG Düsseldorf, 4 O 198/97, GRUR Int 1999, 775 ('Impstoff II'); Christian von Bar, *Internationales Privatrecht*, vol II (2nd edn, CH Beck 1991) 518; James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 151.

within the scope of Article 5(3). In *Mölnlycke AB v Procter & Gamble Ltd*, Dillon LJ in the Court of Appeal, stated that 'It is not in doubt that patent infringement falls within the rubric of Article 5(3), "matters relating to tort, delict or quasi-delict".'³⁰⁰ Five years later, the same point was made in relation to copyright infringement by Lloyd J in *Pearce v Ove Arup Partnership Ltd*,³⁰¹ a case involving copyright over architectural plans and that decision was affirmed by the Court of Appeal in *Fort Dodge Animal Health Ltd v Akzo Nobel NV*.³⁰² In *Pearce*, Lloyd J stated as follows:

'An action for breach of copyright is plainly within the scope of the civil and commercial matters to which the Convention applies'.³⁰³

In addition, there are French decisions applying Article 5(3) in relation to copyright infringement³⁰⁴ and a German one applying Article 5(3) in relation to trade mark infringement.³⁰⁵

³⁰⁰ *Mölnlycke AB v Procter & Gamble Ltd* [1992] 1 WLR 1112, 1117.

³⁰¹ *Pearce v Ove Arup Partnership Ltd* [1997] Ch 293 (Lloyd J). Incidentally, this was the first case in which infringement of a foreign proprietary intellectual property right was asserted in the English courts under the old Brussels Convention. Stated differently, it was the first case where an English court had to decide whether the subject matter limitation in respect of foreign intellectual property rights under the traditional English rules applied in a Brussels Convention case. James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 215. In *Pearce*, the plaintiff alleged that two Dutch defendants had infringed his copyright in architectural plans for a building, drawn up in England, by copying them in designing a building in the Netherlands. It was also alleged that the civil engineers retained for the construction of the building and the owner of the building infringed his copyright.

³⁰² *Fort Dodge Animal Health Ltd v Akzo Nobel NV* [1998] FSR 222.

³⁰³ *Pearce v Ove Arup Partnership Ltd* 1997] Ch 293, 301 (Lloyd J).

³⁰⁴ See *Ideal Clima SpA v SA Ideal Standard Gaz Pal* [1982], Somm, 378; D Series I-5.3-B13, Cour d'Appel Paris; *Wegmann v Société Elsevier Science Ltd* [1997] IL Pr 760, Cour de Cassation; James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 151.

³⁰⁵ See German Federal Supreme Court, BGH I ZR 201/86, EEC 1988, 415; NJW 1988, 1466; GRUR 1988, 483 (Re Jurisdiction in Tort and Contract); James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 151.

4.2.3 *Important case law relating to Article 5(3)*

Before dealing with the new wording of Article 5(3) under Brussels I, it is important to set out important case law handed down by the ECJ regarding the interpretation of Article 5(3) of the Brussels Convention 1968. There has been at least one judicial exhortation that the Brussels I Regulation should be interpreted in the light of the substantial body of case law decided under the Brussels Convention.³⁰⁶ This would make eminent sense as many of the rules in the Regulation are the same as those in the Convention and their meaning has been previously explained by the Court of Justice following a preliminary reference from a Contracting State to the Convention.³⁰⁷

4.2.3.1 *The definition of the term 'tort' under the Brussels regime*

The risk existed of Article 5(3) being given a different scope in different Member States. The Court of Justice dealt with this risk in *Kalfelis v Bankhaus Schröder, Münchmeyer, Hengst and Co* where it held that the meaning of 'matters relating to tort' should not be interpreted solely by reference to national law. It should be regarded as an autonomous concept which 'covers all actions which seek to establish the liability of a defendant and which are not related to a 'contract' within the meaning of Article 5(1).'³⁰⁸ Thus, the terms 'tort, delict or quasi-delict' were given an independent or autonomous meaning under the Brussels Convention. As a consequence, an action can fall within the scope of Article 5(3) even if it is not regarded as tortious by the domestic law of the State where the seised court is located. For the purposes of the application of

³⁰⁶ Case C-281/02 *Owusu v Jackson* [2005] ECR I-1383, Opinion of AG Léger, paras 193 et seq, where he refers to Recital (19) in the Preamble to Brussels I which states the necessity to ensure continuity between the Convention and the Regulation, particularly as regards the interpretation of the Convention by the Court of Justice. AG Léger cautioned against any interpretation of the jurisdiction rules which might mark a departure from the copious case law of the Court concerning the Convention. Such departure, he argued, would constitute a change of direction in the case law which would 'manifestly not be in harmony with the Community legislature's concern to ensure continuity in the interpretation of the two instruments.'

³⁰⁷ James Fawcett, Janeen Carruthers and Peter North, *Cheshire, North & Fawcett: Private International Law* (14th edn, OUP 2008) 207.

³⁰⁸ Case 189/87 *Kalfelis v Bankhaus Schröder, Münchmeyer, Hengst and Co* [1988] ECR 5565, 5585.

the Convention, the concept of 'tort, delict or quasi-delict' must be interpreted principally by reference to the scheme and objectives of the Convention in order to ensure that the latter is given full effect.³⁰⁹

Besides copyright infringement, it has been held that actions for defamation,³¹⁰ negligent misstatement,³¹¹ infringement of foreign intellectual property rights,³¹² passing off,³¹³ unfair competition,³¹⁴ and actionable breaches of EU law giving rise to a claim for damages³¹⁵ all fall within the scope of Article 5(3).³¹⁶

4.2.3.2 *Handelskwekerij G J Bier v Mines de Potasse d'Alsace (the Reinwater case)*

The notion of 'the place where the harmful event occurred' (the old wording of Article 5(3), under the Brussels Convention) was examined by the Court of Justice in *Handelskwekerij G J Bier BV v Mines de Potasse d'Alsace SA*,³¹⁷ (also known as the 'Reinwater' case).

The Jenard Report had deliberately left open the question of whether 'the place where the harmful event occurred' referred to the place where the event giving rise to the damage occurred or the place where the damage actually occurred. This ambiguity, was, to a large extent, resolved in 'Reinwater' - a classic example of a case involving various elements of a tort being split among different States.

³⁰⁹ See generally, Christopher Withers, 'Jurisdiction and Applicable Law in Antitrust Tort Claims' (2002) 6 JBL 250, 259.

³¹⁰ Case C-68/93 *Fiona Shevill, Ixora Trading Inc, Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-415.

³¹¹ *Domicrest v Swiss Bank* [1999] QB 548.

³¹² *Pearce v Ove Arup Partnership Ltd* [1997] Ch 293, reversed by [1999] 1 All ER 769 (CA) and *Fort Dodge Animal Health Ltd v Akzo Nobel NV* [1998] FSR 222.

³¹³ *Modus Vivendi Ltd v British Products Sanmex Co Ltd* [1996] FSR 790; *Mecklermedia Corp v DC Congress GmbH* [1998] Ch 40.

³¹⁴ *Saba Mölnlycke AS v Procter & Gamble Scandinavia Inc* [1997] IL Pr 704 - A Lugano Convention case.

³¹⁵ *Schmidt v Home Secretary* [1995] 1 ILRM 301.

³¹⁶ James Fawcett, Janeen Carruthers and Peter North, *Cheshire, North & Fawcett: Private International Law* (14th edn, OUP 2008) 247.

³¹⁷ Case 21/76 *Handelskwekerij G J Bier BV v Mines de Potasse d'Alsace SA* [1976] ECR 1735.

The plaintiff had a horticultural business near Rotterdam in the Netherlands which drew water for its crops from the river Rhine. Bier's seedlings were damaged by the high salinity of the waters of the Rhine. The defendant, a French mining company domiciled at Mulhouse (Alsace) discharged copious quantities of residual chloride salts into the Rhine from its works. These discharges were considered to be the principal cause of the high salinity, even as far downstream as Rotterdam. The Dutch plaintiffs wished to sue in the Netherlands, so it was necessary to decide on the place where the harmful event occurred.

The case was referred by the Hague Court of Appeal to the ECJ. The latter ruled that Article 5(3) was intended to cover both the place where the damage occurred³¹⁸ and, if different, the place of the event giving rise to it, where the two are not identical.³¹⁹ It follows from the *Bier* ruling that plaintiffs have a wider choice of jurisdiction in transnational tort situations. They may sue in either of two places, the State where the damage occurred, or the State from where the damage originated.³²⁰

In upholding the jurisdiction of the Dutch court, the ECJ stated as follows:

³¹⁸ Briggs argues that ascribing a place to damage can be an artificial exercise, but that the case law offers some guidance. In principle, damage occurs where the damage or loss first materialises, and not, if this is different, where it or its consequence is subsequently felt. He refers to Case C-220/88 *Dumez France SA and Tracoba SARL v Hessische Landesbank* [1990] ECR I-49 as authority for the proposition. Adrian Briggs, *The Conflict of Laws* (2nd edn, OUP 2008) 79 et seq.

³¹⁹ In short, the claimant has a choice where to sue where the places under the causal event limb and the damage limb differ. Oren Bigos, 'Jurisdiction over Cross-Border Wrongs on the Internet' (2005) 54 ICLQ 585, 599.

³²⁰ Interestingly, § 32 ZPO (Section 32 of the German Code of Civil Procedure) adopts a similar approach. Under this Code, the term 'place of infringement' is to be understood as meaning both the place where the act causing the harm was committed and the place where the result occurred (principle of ubiquity). If these places are located in different countries, the injured party is given a choice of forum for the recovery of the entire damages from the multinational act of infringement. This principle was laid down by the Reich Supreme Court in 1936 JW 1291. However, if the defendant is domiciled or has its registered office in a Contracting State to the Brussels Convention/Brussels I, Article 5(3) of Brussels I/Brussels Convention 1968 will take precedence over Section 32 of the Code of Civil Procedure.

[I]t is well to point out that the place of the event giving rise to the damage no less than the place where the damage occurred can, depending on the case, constitute a significant connecting factor from the point of view of jurisdiction. Liability in tort, delict or quasi-delict can only arise provided that a causal connection can be established between the damage and the event in which the damage originates. Taking into account the close connection between the component parts of every sort of liability, it does not appear appropriate to opt for one of the two connecting factors mentioned to the exclusion of the other, since each of them can, depending on the circumstances, be particularly helpful from the point of view of the evidence and of the conduct of the proceedings. To exclude one option appears all the more undesirable in that, by its comprehensive form of words, Article 5(3) of the Convention covers a wide diversity of kinds of liability. Thus, the meaning of the expression ‘place where the harmful event occurred’ in Article 5(3) must be established in such a way as to acknowledge that the plaintiff has an option to commence proceedings either at the place where the damage occurred or the place of the event giving rise to it.³²¹

This wide interpretation was justified by the Court in a number of ways.³²² First, Article 5(3) is concerned to give jurisdiction to an appropriate forum. Both, the place of acting and of damage, are appropriate places for trial. Secondly, it is designed to give the claimant the option of suing elsewhere than in the Contracting State where the defendant is domiciled. Applying a place of acting rule on its own would not normally allow this. Applying a place of damage rule on its own would ignore cases where the act took place somewhere other than in the State where the defendant is domiciled. Thirdly, there is artificiality in concentrating on one element in a tort or delict to the exclusion of the other elements. Fourthly, the Court explained that both the place of acting and the place of damage constitute significant connecting factors that can be particularly helpful

³²¹ Case 21/76 *Handelskwekerij G J Bier BV v Mines de Potasse d’Alsace SA* [1976] ECR 1735, paras 15-19.

³²² James Fawcett, Janeen Carruthers and Peter North, *Cheshire, North & Fawcett: Private International Law* (14th edn, OUP 2008) 253.

from the point of view of the evidence and the conduct of the proceedings.³²³ This fourth point is related to the reason for invoking Article 5(3), described as follows by the ECJ:

'the existence, in certain clearly defined situations, of a particularly close connecting factor between a dispute and the court which may be called upon to hear it, with a view to the efficacious conduct of the proceedings.'³²⁴

At first glance, the interpretation favoured by the ECJ seems to give the plaintiff an excessively wide choice.³²⁵ However, sometimes the courts are willing to circumscribe the plaintiff's choice of jurisdiction. In the English ruling of *Henderson v Jaouen*,³²⁶ *Bier* was distinguished and the exception in Article 5(3) was held not to apply. The respondent, an English citizen, tried to distinguish between original injuries sustained in

³²³ Case 21/76 *Handelskwekerij G J Bier BV v Mines de Potasse d'Alsace SA* [1976] ECR 1735, para 17.

³²⁴ *Ibid* para 11; For implications of the *Bier* ruling, see Andreas F Lowenfeld, Linda J Silberman (eds), *The Hague Convention on Jurisdiction and Judgments – Records of the Conference Held at New York University School of Law on the Proposed Convention, April 30 – May 1, 1999* (Juris Publishing 2001). Again the position on torts understood by most of the world is essentially that established in *Handelskwekerij G J Bier BV v Mines de Potasse d'Alsace*. Most systems consider it fair to summon a defendant either at the place of acting or the place of immediate harm, as opposed to the place where secondary or ripple effects are experienced. The United States however, has a problem, not so much with the place of acting, but with the place of harm unless there has been some 'purposeful availment' on the part of the defendant. Both the European Court and the Supreme Court of the United States are concerned with the same problem: to prevent the defendant being hauled before an unexpected forum. With regard to 'purposeful availment', the piece refers to the following decisions: *Asahi Metal Industry Co Ltd. v Superior Court of California*, 480 US 102 (1987) and *World-Wide Volkswagen v Woodson*, 444 US 286 (1980).

³²⁵ For a ruling which applies the principle in *Bier*, see *Haftpflichtverband der Deutschen Industrie Versicherungsverein auf Gegenseitigkeit (HDI) v Société AXA France IARD* [2007] IL Pr 28, Cour de Cassation. There, the Cour de Cassation confirmed the duality of jurisdiction laid down in *Bier* and held that the damage occurred when defective components (manufactured in Germany) were placed in products. As the defective components had been inserted into products in a workshop in France, it was held that the French courts had jurisdiction (and not the German courts, as argued by the appellant German insurance company).

³²⁶ *Henderson v Jaouen* [2002] EWCA Civ 75 (CA, Wall J).

a road accident in France and a deterioration in his condition which occurred mainly in England. On the basis of the deterioration (harmful event) occurring in England, the respondent argued that the English courts should have jurisdiction to try his claim. The Court of Appeal did not agree. In allowing the appeal, the court stated that the term 'harmful event' was an autonomous Convention concept. Crucially, the court ruled that the subsequent deterioration in the respondent's condition was not a *fresh* tort but, in fact, derived from the original tort. The fact that the deterioration created a fresh cause of action in *French* law was deemed irrelevant as the overriding element was that of the autonomous Convention interpretation of the term 'harmful event'. In sum, the court of appeal ruled against a duality of jurisdiction in this case and found against jurisdiction vesting in the English courts.

Where the harm suffered takes the form of the claimant failing to receive a payment to which he was entitled, the harm occurs at the place where the payment should have been made.³²⁷

Furthermore, in most cases involving a transnational tort, the place of the event giving rise to the damages is likely to coincide with the defendant's domicile.

4.2.3.3 Transnational torts and the extent of jurisdiction of courts

One issue left open by 'Reinwater', was the respective extent of the jurisdiction of the Dutch and French courts insofar as the latter did not derive jurisdiction from the defendant's domicile.

The *Bier* rule was applied by the Court of Justice³²⁸ in the very different context of multi-state defamation in *Fiona Shevill, Ixora Trading Inc, Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA*.³²⁹

Shevill involved libel proceedings in England. The defendants were the French publishers of the newspaper *France Soir*. A number of plaintiffs commenced

³²⁷ *Dolphin Maritime & Aviation Services Ltd v Sveriges Angfartygs Assurans Forening* [2009] 2 Lloyd's Rep 123.

³²⁸ The rationale applied in the *Bier* ruling was followed in Australia. The ruling, by the Federal Court of Australia, is *David Syme Ltd v Grey* (1992) 115 ALR 247.

³²⁹ Case C-68/93 *Fiona Shevill, Ixora Trading Inc, Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-415, paras 19 et seqq.

proceedings against Presse Alliance after one of the defendant's articles seemed to implicate them in illegal activities. Referring the case to the ECJ, the House of Lords sought guidance, *inter alia*, on the interpretation of the phrase 'the place where the harmful event occurred'.

The Court of Justice held that the definition in *Bier* also covered injury to reputation.³³⁰ Accordingly, the plaintiff had the option of suing either in the courts of the place where the damage occurred or in the courts for the place of the event which gave rise to that damage. In other words, the *Shevill* principles permit the plaintiff to bring proceedings in the place where the libel is distributed (place where the damage actually occurs) or in the place where the publisher is established (place where the event giving rise to the damage occurs).³³¹

However, the ECJ drew an important distinction between the fora in terms of the damages that they could award. The courts of the place where the publisher of the defamatory publication is established have jurisdiction to award damages for all the harm caused by the defamation while the courts of each of the Member States in which the publication was distributed (and where the victim claims to have suffered injury to reputation) only have jurisdiction to rule in respect of the harm caused in their particular Member State.³³² Viewed from the perspective of the victim of the defamatory material, he would be significantly better off suing in the Member State where the publisher of the defamatory material is established as he would be able to recover damages for *all* the loss suffered.

The *Shevill* principles³³³ were applied by the French Cour de Cassation in *Wegmann v Société Elsevier Science Ltd*.³³⁴ *Wegmann* was somewhat similar to *Shevill* in that it concerned the infringement of copyright by counterfeiting and involved publications

³³⁰ James Fawcett, Janeen Carruthers and Peter North, *Cheshire, North & Fawcett: Private International Law* (14th edn, OUP 2008) 253.

³³¹ Case C-68/93 *Fiona Shevill, Ixora Trading Inc, Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-415, para 33.

³³² *Ibid.*

³³³ The *Shevill* principles apply whenever there is a tort involving a single causative event in one State and actual harm in a number of other States. Christopher Wadlow, *Enforcement of Intellectual Property in European and International Law* (Sweet & Maxwell 1998) 98.

³³⁴ *Wegmann v Société Elsevier Science Ltd* [1997] IL Pr 760 (CC).

distributed in several Member States. It was held that the victim could pursue its claim for damages either before the courts of the place where the author of the counterfeiting has its establishment (which, following *Shevill*, have jurisdiction to deal with the whole damage), or, under the damage part of Article 5(3), before the courts of the Member States where the counterfeit goods are distributed (which, again, following *Shevill*, have jurisdiction to deal *only* with the damage suffered in that State).³³⁵

In *Domicrest Ltd v Swiss Bank Corp*³³⁶ the tort in question was negligent misstatement. Rix J held that in such a case the place where the harmful event giving rise to the damage occurs is where the misstatement originates, rather than where it is received and relied on. In the case of a telephone conversation between persons in different countries, this is where the words constituting the misstatement are spoken (in the instant case, this was in Switzerland), rather than where they are heard (in the instant case, this was in England). Accordingly, the English court had no jurisdiction. For these purposes, there is no difference between oral or other instantaneous communication and a written document.³³⁷

Rix J refused to follow the earlier negligent misstatement case of *Minster Investments Ltd v Hyundai Precision and Industry Co Ltd*.³³⁸ In that case, which was decided before *Shevill*, Steyn J decided to use a traditional English formula,³³⁹ and ask 'where in substance the cause of action in tort arises, or what place the tort is most closely connected with'.³⁴⁰ The essence of the action for negligent misstatement was said to be the negligent advice and reliance on it. Certificates negligently produced in France and Korea were received and relied upon in England, and accordingly there was jurisdiction in England. However, as Rix J pointed out, the 'substance' test does not reflect either

³³⁵ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) 167 and 168 where the *Wegmann* ruling is discussed along with an analysis of applying *Shevill* in a case of online trade mark infringement (i.e. *Castellblanch SA v Champagne Louis Roederer SA* [2004] IL Pr 41).

³³⁶ *Domicrest Ltd v Swiss Bank Corp* [1999] QB 548.

³³⁷ *Ibid* 567 et seq.

³³⁸ *Minster Investments Ltd v Hyundai Precision and Industry Co Ltd* [1988] 2 Lloyd's Rep 621.

³³⁹ Taken from cases on the old tort head of RSC, Order 11 (now CPR, r 6.20).

³⁴⁰ *Minster Investments Ltd v Hyundai Precision and Industry Co Ltd* [1988] 2 Lloyd's Rep 621.

the wording or the philosophy of the Brussels Convention as laid down in the European Court's decisions.³⁴¹ The *Domicrest* approach has been preferred to that in *Hyundai* by other judges at first instance³⁴² and by Mance LJ in *obiter dicta* in the Court of Appeal.³⁴³

In *Réunion Européenne SA v Spliethoff's Bevrachtingskantoor BV*, Advocate General Cosmas acknowledged that in certain cases it may be difficult or indeed impossible to determine the place where the event giving rise to the damage occurred.³⁴⁴ Such impossibility is illustrated by the facts of the case. A large consignment of pears was shipped in refrigerated containers by the defendant maritime carrier from Australia to the Netherlands, then taken by road to France where the consignee discovered that the goods were damaged. There had been a breakdown in the cooling system in the containers.

The ECJ pointed out that in an international transport operation of this kind, the place where the damage occurred cannot be either the place of final delivery (which can be changed mid-voyage) or the place where the damage was ascertained.³⁴⁵

To permit the claimant (consignee) to bring the actual maritime carrier before the courts for the place of final delivery or before those for the place where the damage was ascertained would in most cases mean attributing jurisdiction to the courts for the place of the plaintiff's domicile, whereas the authors of the Convention demonstrated their opposition to such attribution of jurisdiction otherwise than in cases for which it expressly provides. The European Court was also of the view that such an interpretation

³⁴¹ *Domicrest Ltd v Swiss Bank Corp* [1999] QB 548, 566 et seq.

³⁴² *Raiffeisen Zentral Bank Österreich AG v Alexander Tranos* [2001] IL Pr 9; *Alfred Dunhill Ltd v Diffusion Internationale de Maroquinerie de Prestige* [2002] IL Pr 13 [31]; *Sunderland Marine Mutual Insurance Co Ltd v Wiseman* [2007] EWHC 1460 (Comm).

³⁴³ *ABCI (Formerly Arab Business Consortium International Finance and Investment Co) v Banque Franco Tunisienne* [2003] 2 Lloyd's Rep 146 (CA) [41].

³⁴⁴ Case C-51/97 *Réunion Européenne SA v Spliethoff's Bevrachtingskantoor BV* [1998] ECR I-6511, Opinion of AG Cosmas, para 54, where the Advocate General also states that the harmful conduct may have lasted for the entire voyage but 'it would (...) not be reasonable to require the plaintiff to seise the courts of all the places through which the vessel sailed.'

³⁴⁵ Case C-51/97 *Réunion Européenne SA v Spliethoff's Bevrachtingskantoor BV* [1998] ECR I-6511, para 33-35.

of the Convention would make the determination of the competent court depend on uncertain factors, which would be incompatible with the objective of the Convention which is to provide clear and certain attribution of jurisdiction.³⁴⁶

In such circumstances, the ECJ held that the place where the damage arose in a case involving an international transport operation of the kind at issue (in the main proceedings) can only be the place where the actual maritime carrier was to deliver the goods.³⁴⁷ In the court's view, such place meets the requirements of foreseeability and certainty imposed by the Convention and displays a particularly close connecting factor with the dispute in the main proceedings, so that the attribution of jurisdiction to the courts for that place is justified by reasons relating to the sound administration of justice and the efficacious conduct of proceedings.³⁴⁸ The ECJ went on to specifically exclude the possibility of the place where damage is discovered serving to determine the 'place where the harmful event occurred' within the meaning of Article 5(3) of the Convention, as interpreted by it.³⁴⁹

4.2.3.4 Indirect economic loss cannot found jurisdiction

Indirect financial damage cannot be relied on to found jurisdiction. This principle was laid down in two decisions of the European Court of Justice, namely, *Dumez France SA and Tracoba SARL v Hessische Landesbank*³⁵⁰ and *Marinari v Lloyd's Bank plc*.³⁵¹ The general rule for torts causing economic loss, is that the existence of indirect parasitic damage suffered outside the actual place of infringement or by more than one person,

³⁴⁶ Ibid para 34; Case C-26/91 *Handte v Traitements Mécano-Chimiques des Surfaces* [1992] ECR I-3967, para 19; Case C-364/93 *Marinari v Lloyds Bank plc* [1995] ECR I-2719, para 19.

³⁴⁷ Case C-51/97 *Réunion Européenne SA v Spliethoff's Bevrachtungskantoor BV* [1998] ECR I-6511, para 35.

³⁴⁸ Ibid para 36.

³⁴⁹ Ibid para 37.

³⁵⁰ Case C-220/88 *Dumez France SA and Tracoba SARL v Hessische Landesbank* [1990] ECR I-49, para 22.

³⁵¹ Case C-364/93 *Marinari v Lloyds Bank plc* [1995] ECR I-2719, para 21.

cannot confer jurisdiction under Article 5(3), even if such damage would be recoverable under national law.³⁵²

Following the *Dumez* ruling, the place of damage will be the place where the relevant physical damage or economic loss is directly sustained. The ECJ held that jurisdiction must be limited to where the harmful event 'directly produced its harmful effects upon the person who is the immediate victim of that event' and would not normally cover the domicile of an indirect victim.³⁵³ The facts in *Dumez* were that the German defendant bank had allegedly caused the insolvency of German subsidiary companies of the French plaintiffs. The German subsidiary companies were involved in a building project and the plaintiffs argued that the defendant bank had withdrawn credit facilities from another company on whom the subsidiaries were dependent. Upon withdrawal of the credit, the project came to a halt. The French parent company argued that it had sustained losses at its registered office and commenced actions in the French courts claiming damages against the bank. On a reference from the Cour de Cassation, the ECJ held that Article 5(3) of the Brussels Convention could not be construed as allowing the parent companies to bring proceedings in France against German defendants.

The *Bier* case, although allowing jurisdiction to be assumed in the State where the harm occurs, was concerned with cases where a direct consequence was felt in a Member State (this would be in Germany), not an indirect consequence, as occurred in France.

The European Court pointed out that 'the damage alleged is no more than the indirect consequence of the harm initially suffered by other legal persons who were the direct victims of damage which occurred at a place different from that where the indirect victim suffered harm.'³⁵⁴ The issue therefore, was to decide whether the term 'place where the damage occurred' can cover a place where the indirect victim of the harm discovered the harmful consequences to their own property. The Court decided to limit the application of the term to harm suffered by the immediate victims. The court clarified that while the phrase may refer to the place where the damage occurred, the latter should be taken to mean only the place where the causal event, giving rise to

³⁵² Christopher Wadlow, *Enforcement of Intellectual Property in European and International Law* (Sweet & Maxwell 1998) 101.

³⁵³ Case C-220/88 *Dumez France SA and Tracoba SARL v Hessische Landesbank* [1990] ECR I-49, para 20.

³⁵⁴ *Ibid* para 14.

delictual or quasi-delictual liability, directly produced the harmful effects in relation to the person who is the immediate victim.

The Court summed up its findings as follows:

the rule of jurisdiction laid down in Article 5(3) of the Convention cannot be construed as permitting a plaintiff pleading damage which he claims to be the consequence of the harm suffered by other persons, who were direct victims of the harmful act to bring proceedings against the perpetrator of that act in the courts of the place in which he himself ascertained the damage to his assets.³⁵⁵

The *Dumez* ruling was followed in *Marinari v Lloyds Bank plc* (Zubraidi Trading Co Intervener),³⁵⁶ which was a simpler case involving direct and indirect damage to the same person. In *Marinari*, the Italian domiciled plaintiff was arrested in England and promissory notes were sequestered. The plaintiff subsequently brought an action in Italy, *inter alia*, for compensation for the damage he claimed to have suffered as a result of his arrest, the breach of several contracts and injury to his reputation.

The ECJ held that the place of damage was to be interpreted as not referring to the place where the victim claimed to have suffered financial loss consequential upon initial damage arising and suffered by him in another Member State. The Court of Justice was concerned to keep Article 5(3) within certain bounds so as to avoid multiplication of competent fora.³⁵⁷ It also wanted to avoid the situation where the plaintiff was able to sue in the place where he was domiciled.³⁵⁸ Subsequent rulings followed *Marinari*. For

³⁵⁵ Ibid para 22.

³⁵⁶ Case C-364/93 *Marinari v Lloyds Bank plc* [1995] ECR I-2719.

³⁵⁷ Ibid paras 12-15. The ruling in *Domicrest Ltd v Swiss Bank Corp* [1999] QB 548 is consistent with the judicial reasoning used in *Marinari*.

³⁵⁸ A case in point is Case C-168/02 *Rudolf Kronhofer v Marianne Maier* [2004] ECR I-6009, a preliminary ruling handed down by the ECJ. In *Kronhofer*, the European Court ruled that the phrase 'place where the harmful event occurred' did not refer to the place where the claimant was domiciled or where his assets were concentrated by reason only of the fact that he had suffered financial damage there resulting from the loss of part of his assets that had been incurred in another Member State. Referring to *Marinari*, the court stated at para 19 that the phrase was not to be interpreted so widely that it could include *any* place where adverse consequences were felt of an event which has already caused damage actually arising elsewhere.

example, in *Kitetechnology BV v Uncor GmbH Plastmaschinen*, it was held that in the case of breach of confidence, there is no jurisdiction in the Member State where there is financial loss consequent on the damage to the claimant's commercial interests.³⁵⁹ And, in *Mazur Media Ltd v Mazur Media GmbH*, Mr Justice Collins also ruled against granting jurisdiction to English courts because damage caused by an inability to exploit copyright in sound recordings (due to not having physical possession of the recordings) was the kind of consequential loss (under Article 5(3)) which the court in *Marinari* had already ruled out.³⁶⁰

4.2.4 *The new Article 5(3)*

As stated earlier in this thesis, Article 5(3) deals with torts, delict or quasi-delict. Article 5(3) of Brussels I is virtually identical to Article 5(3) of the Brussels Convention. It states that a person domiciled in a Member State may be sued in another Member State 'in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred *or may occur*'.³⁶¹ In essence, this means that Article 5(3) applies to cases of threatened wrongs as well as wrongs already committed, thereby providing a clear ground of jurisdiction for preventive measures.³⁶² Where, for example, a claimant seeks an injunction to prevent the commission of an online copyright infringement, Article 5(3) confers jurisdiction on the court for the place where the harm would occur if the publication were not prevented.³⁶³

³⁵⁹ *Kitetechnology BV v Uncor GmbH Plastmaschinen* [1994] IL Pr 568, 581 et seq.

³⁶⁰ *Mazur Media Ltd v Mazur Media GmbH* [2004] EWHC 1566 (Ch) [44]-[52], in particular [52].

³⁶¹ The modification introduced by Brussels I appears in bold.

³⁶² Referring to Article 5(3) of Brussels I, Tritton states:

Thus, it makes it clear that *quia timet* actions are triable in the Member State where the harmful event is threatened. It is not clear from 'may occur' as to how immediate the threat must be. In the United Kingdom, a *quia timet* action does not arise unless there is a serious and immediate threat of invasion of the rights of the claimant.

Guy Tritton, *Intellectual Property in Europe* (3rd edn, Sweet & Maxwell 2008) 1176.

³⁶³ CMV Clarkson and Jonathan Hill, *The Conflict of Laws* (4th edn, OUP 2011) 93 (where those authors use the example of another tort, defamation, to demonstrate which court may assume jurisdiction).

The wording of the new Article 5(3) is slightly curious though, since it seems to require the plaintiff to make a choice between the place where the tort was committed and the place where the tort may, at some time in the future, be committed. The use of the word 'or' in the new Article 5(3) seems to make the two possibilities (available to the plaintiff) mutually exclusive. This is unusual since theoretically nothing should stop two or more courts in different Brussels I countries assuming jurisdiction over different parts/elements of an online tort which occur/may occur on their (respective) national territories.

In providing for preventive actions, Brussels I is consistent with the EU intellectual property framework as the Community Patent Convention,³⁶⁴ the Community Trade Mark Regulation,³⁶⁵ and the Community Design Regulation.³⁶⁶ All allocate jurisdiction to the Contracting State in which an act of infringement was committed *or threatened*. Arguably, Article 44 of the TRIPs Agreement also supports the view that jurisdiction can be assumed on the basis of potential threats – it requires judicial authorities to have power to prevent an infringement on their territory.

The new Article 5(3) may have significant implications for jurisdictional issues in instances of digital copyright infringement. Since digital copyright material can be illegally downloaded or disseminated practically anywhere in the world, the amended Article 5(3) introduces a high degree of uncertainty into the equation. Theoretically, the new Article 5(3) enables the plaintiff to issue proceedings in any of the Brussels I Member States, if he believes his copyright may be infringed there.

The new wording of Article 5(3) gives the plaintiff an unlimited choice of forum, delimited only by the geographic scope of application of Brussels I.³⁶⁷ Relating as it

³⁶⁴ Agreement 89/695/EEC relating to Community patents - Done at Luxembourg on 15 December 1989 [1989] OJ L401/1; Protocol on the Settlement of Litigation concerning the Infringement and Validity of Community Patents [1989] OJ L401/34, art 14(5).

³⁶⁵ Council Regulation (EC) 40/94 of 20 December 1993 on the Community trade mark [1994] OJ L11/1, art 93(5).

³⁶⁶ Council Regulation (EC) 6/2002 of 12 December 2001 on Community Designs [2002] OJ L3/1, art 81(a).

³⁶⁷ This unlimited choice of forum is linked to the fact that in an online situation, the defendant has no real control over the location of the damaging act, and perhaps even less control over the location where the damage is suffered. Svantesson analyses this point about lack of

does, to a potential tort, rather than previously committed harm, the new Article 5(3) creates an uncertain basis for jurisdiction and undermines the principle of legal certainty.³⁶⁸

4.2.5 How will the new Article 5(3) operate in practice?

It will be interesting to see how the ‘new’ Article 5(3) operates in practice. It seems that Article 5(3) will entitle the copyright owner to issue proceedings on the basis of a suspected future infringement of his intellectual property rights. In other words, it enables the plaintiff copyright holder to issue proceedings (for example, he may apply for a *quia timet* injunction) in the courts of any of the Brussels I Member States where he believes his copyright may be infringed in the future.

While it might sound odd, it is not implausible (or impossible) for an IP holder to issue proceedings in all 28 Member States on the basis of a mere suspicion about threatened IP infringement. Through the insertion of the words ‘or may occur’ in Article 5(3) of Brussels I, the EU legislators have created a hostage to fortune as twenty-first century technology enables IP infringers to breach or potentially breach copyright transnationally with considerable ease.

Difficulties may arise in relation to Article 5(3) if the defendant is based outside the geographic scope of Brussels I but transmits infringing material to a recipient in a Brussels I Member State.³⁶⁹ If the defendant has significant assets in one of the Brussels

control in the context of Internet defamation and states that it constitutes ‘the very root of the problem of jurisdiction’ in that particular area. Dan Svantesson, ‘Jurisdictional Issues in Cyberspace; At the Crossroads - the Proposed Hague Convention and the Future of Internet Defamation’ (2002) 18 CLSR 191, 193.

³⁶⁸ Concerns have been raised about the risk of forum-shopping linked to the wording of Article 5(3) of the Brussels Convention 1968. For instance, see Commission, ‘Proposal for a regulation of the European Parliament and the Council on the law applicable to non-contractual obligations (“Rome II”)’ COM (2003) 427 final 6.

³⁶⁹ This may not prove troublesome if new proposals to extend the jurisdiction rules of Brussels I to third country defendants are put in place. See: Commission, ‘Proposal for a Regulation of the European Parliament and the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Recast)’ COM (2010) 748 final 8, Recital (16), art 4(2).

I Member States, then it may prove worthwhile trying to attach his assets in that country.³⁷⁰ Other possible complicating factors in respect of the potentially broad prosecutorial scope of Article 5(3) are the Brussels I provisions relating to *lis pendens* and provisional measures.

4.2.6 *Lis Pendens*

Section 9 (Articles 27 to 30 inclusive) of Brussels I relates to *Lis Pendens* (or related actions). Arguably, the most relevant provision in this Section is Article 28. It states that where related actions³⁷¹ are pending in the courts of different Member States, any court other than the court first seised may stay its proceedings.³⁷² Also, it is open to one of the parties to the action to apply to any court *other than* the court first seised to decline jurisdiction if the court first seised has jurisdiction over the actions in question and its law permits the consolidation thereof.³⁷³ Under Brussels I, actions are deemed to be

³⁷⁰ Under the Commission Proposal (see previous fn) it is provided that a non-EU defendant can be sued at the place where moveable assets belonging to him are located provided their value is not disproportionate to the value of the claim and that the dispute has a sufficient connection with the Member State of the court seised.

³⁷¹ For a British ruling on the notion of 'related actions' see *Research in Motion UK Ltd v Visto Corporation* [2008] EWCA Civ 153 [25] et seqq. There, the Court of Appeal had to decide whether English proceedings and Italian proceedings concerning revocation and declaration of non-infringement proceedings (patent) were related for the purposes of Article 28 Brussels I. Citing the House of Lords case *Sario v Kuwait Investment Authority* [1999] 1 AC 32, the Court of Appeal referred at para [28] of its ruling to Lord Saville's speech in *Sario* [40] et seq in which he propounded a broad test for 'related actions' based on a common sense approach rather than an over-sophisticated analysis of the matter which would be complicated by the fact that the court would be dealing not with actual judgments, but with what judgments yet-to-be-given would contain. Rochelle C Dreyfuss and Jane C Ginsburg, 'Draft Convention on Jurisdiction and Recognition of Judgments in Intellectual Property Matters' (WIPO Forum on Private International Law and Intellectual Property, WIPO/PIL/01/7, 2001), Article 13(2) provided that (for the purposes of that particular provision/article) actions are deemed to be related where, irrespective of the territorial scope of the rights and the relief sought, the claims arise out of the same transaction or series of transactions or occurrence. Article 13(2) is titled 'Consolidation of Territorial Claims'.

³⁷² Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1, art 28(1).

³⁷³ *Ibid* art 28(2).

related where they are so closely connected that it is expedient to hear and determine them together to avoid the risk of irreconcilable judgments resulting from separate proceedings.³⁷⁴ Article 30 of Brussels I sets out the conditions that have to be satisfied for a court to be deemed to be seised of an action.

If a copyright infringer (defendant in an Article 5(3) action) were a corporate with a presence in a number of Brussels I Member States, it would be appropriate for him to take a *lis pendens* application under Article 28(2), Brussels I, seeking the court second seised to decline jurisdiction.

The existence of this mere possibility or risk of infringement is sufficient to satisfy the 'may occur' part of the newly worded Article 5(3), thereby entitling the copyright holder to issue court proceedings in all of the Brussels I countries if he so wishes. However, the concept of legal certainty is undermined by two things, the fact that the new Article 5(3) captures future *potential* torts and, the much greater likelihood of transnational torts occurring (due to the internet).

And what if the plaintiff's suspicions prove unfounded in all or a majority of the countries? Considerable court time and resources will have been expended and jurisdiction may have been assumed by a number of courts, all in vain.³⁷⁵ There was a time when *quia timet* jurisdiction was viewed as little more than an interesting possibility but now, under the new Article 5(3), it is a reality.

³⁷⁴ Ibid art 28(3).

³⁷⁵ Article 27 of Brussels I (the *Lis Pendens*, or related actions provision) may assist here. Article 27(1) provides that where proceedings involving the same cause of action and between the same parties are brought in the courts of different Member States, any court other than the court first seised shall of its own motion stay its proceedings until such time as the jurisdiction of the court first seised is established. Article 27(2) provides that where the jurisdiction of the court first seised is established, any court other than the court first seised shall decline jurisdiction in favour of that court. The usefulness of Article 27(1) may be diminished where the plaintiff copyright holder decides to instigate proceedings simultaneously in all the relevant jurisdictions. In that scenario, there is a risk that many courts become seised of the matter simultaneously or virtually simultaneously.

4.2.6.1 Provisional Measures

Under Article 31, Brussels I, application may be made to the courts of a Member State for such provisional, including protective measures as may be available under the law of that State even if, under this Regulation, the courts of another Member States have jurisdiction as to the substance of the matter.

While this provision does not relate to jurisdiction issues *per se*, it does give potential applicant copyright holders some added rights/powers in terms of IP protection. Article 31 does not seem to preclude the possibility of applicants applying to the courts of a number of Member States simultaneously for provisional/protective measures.

According to the Court of Justice, 'provisional protective measures' under Article 24 of the Brussels Convention (which corresponds to Article 31 of Brussels I) are ones which are intended to maintain a legal or factual situation in order to safeguard rights.³⁷⁶ Such measures encompass the English freezing (*Mareva*) injunction and search (*Anton Piller*) order, the Continental *saisie conservatoire*, an ordinary interlocutory injunction under English law³⁷⁷ and a French process of appointing a judicial expert, who investigated and protected evidence of facts but could not impose any final solution of the dispute on the parties, regarded by French law as interim proceedings.³⁷⁸

In *De Cavel v De Cavel*,³⁷⁹ Article 31 was interpreted by the Court of Justice as only applying to provisional measures which relate to matters within the scope of the Regulation. It has to be asked what rights a provisional measure seeks to protect and, if these rights are outside the scope of the Regulation, a provisional measure cannot be granted under Article 31.

³⁷⁶ Case C-261/90 *Mario Reichert, Hans-Heinz Reichert and Ingeborg Kockler v Dresdner Bank* [1992] ECR I-2149.

³⁷⁷ See *Kitechnology BV v Unicor GmbH Plastmaschinen* [1994] IL Pr 568 (CA).

³⁷⁸ *Miles Platts Ltd v Townroe Ltd* [2003] EWCA Civ 145.

³⁷⁹ Case 143/78 *De Cavel v De Cavel* [1979] ECR 1055.

A party may seek interim relief under Article 31 even if the main proceedings in the other Member State have not actually started. All that is required is that the possibility of substantive proceedings exists under national law.³⁸⁰

4.3 Conclusions

Jurisdiction and more particularly, the Brussels I Regulation, have formed the core of this chapter. Within Brussels I, Articles 2 and 5(3) carry most relevance to this thesis.

Article 5(3), a special jurisdiction provision, is, in effect an exception to the basic rule contained in Article 2. By way of the ‘Reinwater’ ruling, the ECJ gave the plaintiff a wide choice of jurisdiction where a transnational tort is perpetrated. In essence, where the tort is split among different States, the plaintiff may sue in either of two places: the State where the damage occurred or the State from where the damage originated. Transplanting that principle to an online copyright infringement scenario, it would seem that the prejudiced copyright holder could sue in either the courts of the country where the copyright-protected content was illegally copied or in the courts of the country where his economic or moral rights were negatively affected.

The ‘new’ Article 5(3) containing the potentially problematical phrase ‘or may occur’ as implemented by Brussels I applies to cases of threatened wrongs and provides a clear ground of jurisdiction for preventive measures. In a way, one could provocatively argue that the EU legislators, when devising the new Article 5(3), overlooked the heightened threat/risk posed to digital content by the internet. As digital copyright material can be copied and disseminated (illegally) with considerable ease in the twenty-first century, one could argue forcefully that the EU legislature has given a hostage to fortune. Under Article 5(3), potential claimants could apply for a *quia timet* injunction in any Member State where they fear their copyright will be infringed. While admittedly improbable, it is certainly not impossible for a potential claimant to bring *quia timet* proceedings in all 28 Member States. Under current proposals to revise Brussels I, defendants domiciled in third countries would also fall within the scope of Brussels I meaning that even more jurisdictional optionality would be given to the would-be claimant.

³⁸⁰ Case C-391/95 *Van Uden Maritime BV (t/a Van Uden Africa Line) v Kommanditgesellschaft in Firma Deco-Line* [1998] ECR I-7091, paras 29, 48. In this case it was enough that proceedings ‘may be commenced’.

Nor should it be accepted as a given that the *Lis Pendens* provision of Brussels I will provide a definitive solution as Article 27, Brussels I only applies where the same parties are in litigation in different Member States. It is this provision which requires the court second seised to stay its proceedings. Where threatened torts are envisaged in different countries, it is unlikely that the same potential defendant will be involved in all of them.

After Article 27, Brussels I, the next most likely related actions provision to apply is Article 28 but that provision contains no obligation on the second seised court to stay its proceedings. It states that the second seised court *may* stay its proceedings. In brief, therefore, parallel preventive proceedings may occur in a number of Member States (and, in the future, third States, potentially) without any automatic solution emanating from the related actions provisions.

On the EU front, there now exists, for the first time ever, an applicable law framework for non-contractual obligations (Rome II) while Brussels I and Rome I have modernised the jurisdiction and applicable law legislative frameworks, respectively. In terms of the jurisdictional element, the addition of the words 'or may occur' to the wording of the old Article 5(3), Brussels Convention (1968), is arguably a lot more significant than many commentators realise. The amended Article 5(3) creates a new ground of jurisdiction for preventive measures, but as Tritton observes, it is not entirely clear how immediate the threatened action must be.³⁸¹ Conceivably, there may be different conditions to be fulfilled in the Member States in terms of granting a *quia timet* injunction. For instance, in the UK, a *quia timet* action does not arise unless there is a serious and immediate threat of invasion of the rights of the claimant.³⁸²

As twenty-first century technology enables copyright infringers to infringe remotely and disseminate infringing material (widely) with lightning speed, the amended Article 5(3), covering as it does, *potential* torts, creates an uncertain basis for jurisdiction and undermines the principle of legal certainty. Theoretically, under the new Article 5(3), there is nothing to stop a claimant bringing proceedings simultaneously in all 28 Member States. While this eventuality may be improbable, it is not impossible.

³⁸¹ Guy Tritton, *Intellectual Property in Europe* (3rd edn, Sweet & Maxwell 2008) 1176.

³⁸² *Ibid.*

Chapter 5. Private International Law – The Applicable Law

TABLE OF CONTENTS

5.1	Introduction.....	132
5.2	The Applicable Law	133
5.2.1	The Rome II Regulation	133
5.2.2	Specific Rules for Special Torts	135
5.2.3	Article 8 of Rome II and the Infringement of IPRs.....	135
5.3	The Berne Convention for the Protection of Literary and Artistic Works	138
5.3.1	Differing Views on the Actual Meaning of Article 5(2) of the Berne Convention.....	140
5.4	The Rule of Origin versus the Rule of Reception.....	146
5.4.1	The Satellite and Cable Directive.....	147
5.5	The European Commission’s 1995 Green Paper on Copyright	151
5.6	Advantages Associated with the Country of Origin Rule	153
5.7	Disadvantages Associated with the Country of Origin Rule.....	155
5.8	Points of Attachment	157
5.9	An Alternative – The Law of the Country of Reception	159
5.10	Conclusions.....	161

5.1 Introduction

As stated at the beginning of Chapter 4, the jurisdictional and applicable law elements would be dealt with separately in this thesis. For that reason, I am devoting this chapter to the treatment of the applicable law elements having used the previous chapter to treat jurisdictional issues. In this way, an analytical balance is maintained even though a demarcation is drawn between jurisdiction and the applicable law.

In legal proceedings involving a conflict of laws, invariably, both jurisdiction and the applicable law have to be decided by the presiding judge. While the applicable law issue is, relatively speaking, less controversial than the issue of jurisdiction, it is still nonetheless important and needs to be covered to ensure this thesis is both complete and balanced. The landmark Rome II Regulation³⁸³ receives significant attention in this chapter as it governs the applicable law in non-contractual e.g. tortious situations, the Rome I Regulation³⁸⁴ as it becomes relevant where there is concurrent liability (tortious and contractual). Practically speaking, it is important that Rome I is examined in this thesis as it constitutes the third side of the EU conflicts triangle (Brussels I and Rome II constituting the two other sides).

Part of this chapter is also given over to analysis of Article 5(2) of the multilateral Berne Convention and the various interpretations of that provision.

The other applicable law elements dealt with are the SatCab Directive³⁸⁵ (which contains a rule of origin), the merits and demerits of applying a country of origin rule, contrasting the rule of origin with the rule of reception, the European Convention relating to questions on Copyright Law and Neighbouring Rights in the Framework of Transfrontier Broadcasting by Satellite 1994, the European Commission's 1995 Green

³⁸³ Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40.

³⁸⁴ Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6.

³⁸⁵ Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15.

Paper on Copyright and general choice of law rules and theories,³⁸⁶ some of which were specifically formulated for the online world.

5.2 The Applicable Law

Generally speaking, private international law involves a two stage process. The two stages of jurisdiction and the applicable law are not entirely separate and it is becoming increasingly common that a decision on the applicable law be reached at the jurisdictional stage of the process.³⁸⁷ The two stage process is not always evident since reported cases normally only deal with either jurisdiction or the applicable law, but not both of them.

The first element to be determined is the relevant forum. In other words, which court will exercise jurisdiction in the proceedings. Secondly, the court must decide which law will be applied in the proceedings - its own (i.e. the *lex fori*), or that of some other jurisdiction. This is called the applicable law, or choice of law.

5.2.1 The Rome II Regulation

Introduction

Regulation (EC) 864/2007 on the law applicable to non-contractual obligations (Rome II)³⁸⁸ was adopted on 31 July 2007. Its aim is to establish uniform choice of law rules in respect of non-contractual obligations³⁸⁹ arising out of a tort or delict. The Regulation applies to all the Member States except Denmark³⁹⁰ and the substantive scope and the

³⁸⁶ Commission, 'Green Paper: Copyright and Related Rights in the Information Society' COM (1995) 382 final.

³⁸⁷ James Fawcett, 'The Interrelationships of Jurisdiction and Choice of Law in Private International Law' (1991) 44 Current Legal Problems 39.

³⁸⁸ Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40.

³⁸⁹ As the concept of a non-contractual obligation varies from one Member State to another, it should be understood as an autonomous concept for the purposes of Rome II. Regulation (EC) 864/2007 of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40, recital (11).

³⁹⁰ Ibid art 1(4) and recital (40).

provisions of the Regulation should be consistent with Brussels I and the instruments dealing with the law applicable to contractual obligations.³⁹¹

In many ways, Rome II is a landmark in private international law. It is the first EU instrument of general application harmonizing rules of applicable law and it is the most comprehensive instrument of its kind anywhere in the world.³⁹² With its younger sibling, the Rome I Regulation (adopted in June 2008) and with the Brussels I Regulation, it forms a substantial part of a community rulebook that now covers much of the legal territory formerly occupied by national private international law rules in civil and commercial matters.

Rome II has been in force since 11 January 2009.³⁹³ The rationale behind Rome II is spelt out in Recital (6) which states as follows:

The proper functioning of the internal market creates a need, in order to improve the predictability of the outcome of litigation, certainty as to the law applicable and the free movement of judgments, for the conflict of law rules in the Member States to designate the same national law irrespective of the country of the court in which an action is brought.

The set of rules contained in Rome II creates a flexible framework of conflict of laws rules which, in turn, enables the court seised to treat individual cases in an appropriate manner. The regulation provides for the connecting factors which are the most appropriate to achieve these objectives. Therefore, it provides for a general rule but also for specific rules and in certain provisions, for an ‘escape clause’ which allows a departure from these rules where it is clear from all the circumstances of the case that the tort/delict is manifestly more closely connected with another country.³⁹⁴

³⁹¹ Ibid recital (7).

³⁹² Andrew Dickinson, *The Rome II Regulation – The Law Applicable to Non-Contractual Obligations* (1st edn, OUP 2008) Preface.

³⁹³ Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40, art 32. Article 29 is excepted. It entered into force on 11 July 2008 (Article 32).

³⁹⁴ Ibid recital (14).

5.2.2 *Specific Rules for Special Torts*

Articles 5 to 9 of Rome II set out specific rules for special torts.³⁹⁵ One of the special torts covered is the infringement of intellectual property rights, while the others include: product liability, unfair competition, acts restricting competition, environmental damage and industrial action. The use of specific rules for special torts follows the model adopted in a number of European civil law jurisdictions and the US (under its Restatement (Second) of Conflict of Laws (1971)).

In the United Kingdom, the case for having in the Regulation some of these specific rules was not thought to have been made out.³⁹⁶ The European Parliament was also unconvinced and unsuccessfully sought the deletion of some of these rules.³⁹⁷

5.2.3 *Article 8 of Rome II and the Infringement of IPRs*

Article 8 provides specific rules for infringement of IPR. Infringement was regarded as a special tort because of the significance given under both the Berne Convention for the Protection of Literary and Artistic Works of 1886 and the Paris Convention for the Protection of Industrial Property of 1883 to the territoriality principle which attaches great importance to the law of the country in which protection is claimed.³⁹⁸

Article 8 sets out two separate choice of law rules, the first rule is set out in Article 8(1), the second in Article 8(2). Article 8(1) relates to intellectual property rights while Article 8(2) relates to *unitary* Community intellectual property rights. Article 8(3) precludes the law applicable under Article 8 to be derogated from by an agreement under Article 14.³⁹⁹

³⁹⁵ Ibid recital (19) states that ‘Specific rules should be laid down for special torts/delicts where the general rule does not allow a reasonable balance to be struck between the interests at stake.’

³⁹⁶ European Union Committee, *The Rome II Regulation* (HL 2003-04, 66) paras 106 (referring to product liability), 109 (unfair competition) and 134 (violation of the environment).

³⁹⁷ I.e. the specific rules for unfair competition and acts restricting free competition.

³⁹⁸ Commission, ‘Proposal for a regulation of the European Parliament and the Council on the law applicable to non-contractual obligations (“Rome II”)’ COM (2003) 427 final 20.

³⁹⁹ Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40, art 14 permits the parties to submit non-contractual obligations to the law of their choice:

Under Article 8(1), the law applicable to a non-contractual obligation arising from an infringement of an IPR (other than a unitary Community IPR) is the law of the country for which protection is claimed.⁴⁰⁰ For the purposes of the Regulation, the term ‘intellectual property rights’ is to be interpreted as meaning, for instance, copyright, related rights, the *sui generis* right for the protection of databases and industrial property rights.⁴⁰¹ The slightly outmoded term ‘industrial property’ covers, among other things, trade marks and patents.⁴⁰²

Article 8(1) must be read in conjunction with the first sentence of Recital (26) of the Regulation which states as follows:

-
- (a) by an agreement entered into *after* the event giving rise to the damage occurred; or
 - (b) where all the parties are pursuing a commercial activity, also by an agreement freely negotiated *before* the event giving rise to the damage occurred.

The choice must be expressed or demonstrated with reasonable certainty by the circumstances of the case and must not prejudice the rights of third parties.

⁴⁰⁰ It would seem that issues relating to the validity of the IPR, and to its ownership do not fall within Article 8(1). Article 8(1) is only concerned with determining the law applicable to infringement. Lord Collins of Mapesbury et al (eds), *Dicey, Collins and Morris: The Conflict of Laws*, vol 2 (15th edn, Sweet & Maxwell 2012) para 35-074. Interestingly, the ALI used the same wording as Article 8(1) of Rome II in American Law Institute, *Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes* (ALI Publishers 2008) s 301(1)(b) (‘Territoriality’). The ALI eschewed the formulation ‘country *where* protection is sought’ because of its ambiguous meaning: it might mean that the *lex fori* applies or that the *lex loci delicti* applies.

⁴⁰¹ Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40, recital (26). By employing the term ‘for instance’, the European legislator seems to imply that the list is not exhaustive. It is likely that the meaning of intellectual property rights will be developed by reference to a principle of autonomous interpretation. Lord Collins of Mapesbury et al (eds), *Dicey, Collins and Morris: The Conflict of Laws*, vol 2 (15th edn, Sweet & Maxwell 2012) para 35-076.

⁴⁰² Paris Convention for the Protection of Industrial Property 1983, art 1(2) provides as follows: ‘The protection of industrial property has as its object patents, utility models, industrial designs, trademarks, service marks, trade names, indications of source or appellations of origin, and the repression of unfair competition.’

‘Regarding infringements of intellectual property rights, the universally acknowledged principle of the *lex loci protectionis* should be preserved.’

The suggestion that the *lex loci protectionis* is a ‘universally acknowledged principle’ perhaps goes too far.⁴⁰³ Indeed, prior to the Regulation, there was no consistent practice even among the Member States.⁴⁰⁴ The ‘principle’ however, would appear to originate in the idea that IPRs are sovereign in character and operate within territorial limits, with each State having the exclusive power to regulate such rights within its territory.⁴⁰⁵

The argument based on sovereignty and territoriality appears to have exerted a strong influence on the development of Article 8(1) of Rome II. This becomes evident from a reading of the European Commission’s Explanatory Memorandum to the Proposal for Rome II, where the following is stated:

The treatment of intellectual property was one of the questions that came in for intense debate during the Commission’s consultations. Many contributions recalled the existence of the universally recognised principle of the *lex loci protectionis*, meaning the law of the country in which protection is claimed on which e.g. the Berne Convention for the Protection of Literary and Artistic Works of 1886 and the Paris

⁴⁰³ Anette Kur, ‘Applicable Law: An Alternative Proposal for International Regulation – The Max-Planck Project on International Jurisdiction and Choice of Law’ (2005) 30 *Brook J Int L* 951. Also, Lord Collins of Mapesbury et al (eds), *Dicey, Collins and Morris: The Conflict of Laws*, vol 2 (15th edn, Sweet & Maxwell 2012) para 35-078, where the description of the *lex loci protectionis* as being a ‘universally acknowledged principle’ is deemed extravagant.

⁴⁰⁴ Marta Pertegás, ‘Intellectual Property and Choice of Law Rules’ in Alberto Malatesta (ed), *The Unification of Choice of Law Rules on Torts and Other Non-Contractual Obligations in Europe* (CEDAM 2006) 221, 229 – 235.

⁴⁰⁵ Andrew Dickinson, *The Rome II Regulation – The Law Applicable to Non-Contractual Obligations* (1st edn, OUP 2008) 457. Also, Lawrence Collins et al, *Dicey, Morris & Collins on The Conflict of Laws* (14th edn, Sweet & Maxwell 2006) para 22-051, where the following is stated:

The essence of an intellectual property right is the owner’s right to take action to prevent others from engaging in certain types of activity in a given territory without the owner’s permission. Although patents, trade marks and copyright are classified as movables, they share some of the characteristics of immovables in the sense that the rights which they confer are territorially limited.

Convention for the Protection of Industrial Property of 1883 are built. This rule, also known as the ‘territorial principle’, enables each country to apply its own law to an infringement of an intellectual property right which is in force in its territory: counterfeiting an industrial property right is governed by the law of the country in which the patent was issued or the trademark or model was registered; in copyright cases, the courts apply the law of the country where the violation was committed. This solution confirms that the rights held in each country are independent.⁴⁰⁶

5.3 The Berne Convention for the Protection of Literary and Artistic Works

There is a certain symmetry between Rome II (Article 8(1)) and the Berne Convention (Article 5(2)). While there is not absolute consensus that Article 5(2) actually constitutes a formal rule, some, such as Fawcett and Torremans argue that it espouses the *lex loci protectionis*. This section of the thesis will be used to analyse the differing viewpoints on the actual meaning of Article 5(2), Berne Convention.

The Berne Convention’s relevance to this work lies in its Article 5(2) which has been interpreted by many as an applicable law rule. It should be noted that Article 14bis(2)(a) of the Berne Convention also designates the applicable law, but for a very narrow class of works, i.e. cinematographic works. In addition, it only governs copyright *ownership* issues in relation to such works. As a consequence, this particular provision has very limited relevance to this thesis.

The convention’s relevance is increased by the fact that it is the oldest of the international copyright conventions, having been adopted in 1886.⁴⁰⁷ The Berne Convention creates a union comprising all the signatory states. From its inception, the Berne Convention has combined two different techniques: substantive supranational minimum rules and national treatment.⁴⁰⁸ The main basic principles of the Berne

⁴⁰⁶ Commission, ‘Proposal for a regulation of the European Parliament and the Council on the law applicable to non-contractual obligations (“Rome II”)’ COM (2003) 427 final, art 8.

⁴⁰⁷ The Convention has been revised on a number of occasions - in Berlin (1908), in Rome (1928), in Brussels (1948), in Stockholm (1967) and most recently by the Paris Act, 24 July 1971. It was also amended on 29 September 1979.

⁴⁰⁸ Sam Ricketson and Jane Ginsburg, *International Copyright & Neighbouring Rights - The Berne Convention and Beyond*, vol II (2nd edn, OUP 2006) 1297; Roberto Mastroianni, *Diritto Internazionale e Diritto d’Autore* (A Giuffrè 1997) 89 describes national treatment

Convention are those of national treatment⁴⁰⁹ and a guarantee of certain moral rights (attribution and integrity) and economic rights (reproduction, public performance, broadcasting, etc.).⁴¹⁰ Both principles may be invoked by authors to protect their rights. There are 167 contracting parties (countries) to the Berne Convention.⁴¹¹ In addition to regulating the copyright relations between these States, it also provides international standards of protection for all WTO member states, whether or not they are members of the Berne Convention.

Some commentators argue that Article 5(2) of the Berne Convention is a choice of law provision.⁴¹² It provides as follows:

and substantive treaty minima, *jus conventionis*, as the two ‘pillars’ on which the Berne Convention rests.

⁴⁰⁹ The principle of national treatment is common to both the Berne Convention (art 5(1)) and the 1883 Paris Convention for the Protection of Industrial Property (art 2(1)). Under this principle, each member of the Union grants nationals of other Member States the same treatment as it grants its own nationals. JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) para 3.34. Grosheide raises the much debated question of whether the principle of national treatment can also be construed as a private international law rule. He looks at both sides of the argument. From a conflicts perspective, the principle of national treatment leads to the adoption of *the lex protectionis* (or *lex fori*) as the applicable law when a court has to rule on an infringement or existence of rights within its territory. The other side of the argument is that the principle of national treatment provides no conflict of laws rule at all. In cases in which a court is concerned with the existence or infringement of rights within its territory, the national treatment principle ensures only that that country’s domestic law may govern - national treatment accords mandatory status to the *lex protectionis*. Willem Grosheide, ‘Experiences in the Field of Intellectual Property’ in Katharina Boele-Woelki and Catherine Kessedjian (eds), *Internet, Which Court Decides? Which Law Applies?* (Quel tribunal décide? Quel droit s’applique?) (1st edn, Kluwer Law International 1998).

⁴¹⁰ JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) para 18.01.

⁴¹¹ WIPO, ‘Contracting Parties’

<http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15> accessed 29 May 2014.

⁴¹² But this viewpoint is not unanimous, e.g. van Eechoud expresses reservations about whether Article 5(2), Berne Convention is in fact a real choice of law rule. She states as follows in her doctoral thesis:

‘the extent of protection, as well as the means of redress afforded to the author to protect his rights shall be governed exclusively by the laws of the country where protection is claimed.’

It is important to make a few preliminary points about Article 5(2), Berne Convention.

First, it should be noted that there is not absolute consensus that Article 5(2) actually constitutes a formal conflict of laws rule. However, even among the doubters, there is a view that, *in practice*, this provision generally leads to the application of the principle of territoriality, under which the law of each country where the infringement allegedly occurs determines protectability, scope and relief.⁴¹³

Secondly, the expressions ‘extent of protection’ and ‘means of redress ... to protect his rights’ appear to limit the application of Article 5(2) to actual infringement proceedings which are brought to enforce the rights protected under the Convention. This means that this provision will not cover all issues of international copyright, notably, questions of authorship, initial ownership and transfers of ownership.⁴¹⁴

5.3.1 Differing Views on the Actual Meaning of Article 5(2) of the Berne Convention

The phrase ‘the country where protection is claimed’ is ambiguous and it is probably an open question as to whether the phrase refers to the country in which the action is brought,⁴¹⁵ or the country in respect of whose law protection is being claimed (which

The only true conflict rule in the BC [sic] is in my opinion Article 14bis(2c), which clearly provides that the law applicable to the form of an agreement or promise between a (creative) contributor to a film and the producer of the film, is governed by the law of the country in which the producer resides.

Mireille van Eechoud, *Choice of Law in Copyright and Related Rights – Alternatives to the Lex Protectionis* (1st edn, Kluwer Law International 2003) 127.

⁴¹³ Sam Ricketson and Jane Ginsburg, *International Copyright & Neighbouring Rights - The Berne Convention and Beyond*, vol I (2nd edn, OUP 2006) 319, fn 289.

⁴¹⁴ *Ibid* and vol II, 1299. For a comparison of US and UK approaches, see e.g. Paul Goldstein, *International Copyright: Principles, Law and Practice* (OUP 2001) 91-94.

⁴¹⁵ Van Eechoud concedes that only a few writers are of the opinion that Article 5(2) points to the law of the country where the court is seised (*lex fori*) even though a literal reading of the

may not necessarily be the country where the action is brought).⁴¹⁶ Article 5(2) would have more clearly designated application of the law of the place of the infringement had it provided for application of the ‘laws of the country *for which* protection is claimed’ (or, even more clearly, laws of *each* country for which protection is claimed).⁴¹⁷

Both the English and French texts of the Convention clearly state ‘where’ (‘où’), however, which suggests that it may simply have been assumed, that suit would be brought in the country in which the infringement allegedly occurred.

last fourteen words of the provision would seem to support the *lex fori*. Two writers who support the *lex fori* view are: Gustave Huard, *Étude sur les modifications apportées à la Convention de Berne par la conférence réunie à Paris du 15 avril au 1^{er} mai, 1896* (Pichon 1897); and Stephen M Stewart, *International Copyright and Neighbouring Rights* (2nd edn, Butterworths 1989). These works are referred to in Mireille van Eechoud, *Choice of Law in Copyright and Related Rights – Alternatives to the Lex Protectionis* (1st edn, Kluwer Law International 2003) 103, fn 290.

⁴¹⁶ JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 145, fn 39. For the WIPO viewpoint, see that organisation’s IP Survey ‘The Role of Private International Law and Alternative Dispute Resolution’ <http://www.wipo.int/copyright/en/ecommerce/ip_survey/chap4.html#_ftn432> accessed 1 July 2012, where it is stated that while there is hesitation about whether the term ‘country where protection is claimed’ should be read to refer to the forum (i.e. the country where the court proceedings are brought) or the country where the infringing acts have occurred. The latter interpretation is more widely accepted. In making this assertion, the survey cites the following: Jane C Ginsburg, ‘Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks’ (WIPO Forum on Private International Law and Intellectual Property, GCPIC/2, 1998) 35; André Lucas, ‘Private International Law Aspects of the Protection of Works and of the Subject Matters of Related Rights Transmitted over Digital Networks’ (WIPO Forum on Private International Law and Intellectual Property, WIPO/PIL/01/1 Prov, 2000) 6.

⁴¹⁷ Several commentators have contended that Article 5(2) should be read as meaning ‘country for which protection is claimed.’ André Lucas, ‘Private International Law Aspects of the Protection of Works and of the Subject Matters of Related Rights Transmitted over Digital Networks’ (WIPO Forum on Private International Law and Intellectual Property, WIPO/PIL/01/1 Prov, 2000) 12; Silvia Plenter, ‘Choice of Law Rules for Copyright Infringements in the Global Information Infrastructure: A Never-Ending Story’ (2003) 23 EIPR 313, 317 (stating proposition and citing more sources).

Professor Ulmer has argued that, despite the formulation in Article 5(2), this does not logically imply a reference to the law of the forum (although in most cases, this country will be the same as the country where the infringing act occurred).⁴¹⁸ He contends that, taking general principles of PIL into consideration, it would be consistent for a complete rule of conflict of laws to provide that the protection of IPRs should be governed by the law of the country in whose territory the infringement took place (*lex loci delicti*).⁴¹⁹ And, somewhat ironically, the ambiguity of the Convention's drafting may force national courts to determine the issue for themselves, most probably resulting in the application of the *lex loci delicti*. In most instances, it is likely that national choice of court rules will apply the principle of territoriality, and will therefore restrict the application of local substantive law to infringements committed within their jurisdictions. By the same token, the forum (if it finds the foreign infringement claim justiciable) would apply the laws of the foreign territories concerned to infringements committed abroad.⁴²⁰

Another scenario which highlights the (potential) disjunction between the country *where* protection is claimed, and the country *for which* protection is claimed is the less usual occurrence of an author bringing infringement proceedings in a country other than the country in which infringement was committed.⁴²¹ This decision might be influenced by the physical location of defendant assets which could be used to satisfy any monetary award granted. Such a case might also arise if the plaintiff is bringing in a single forum, claims alleging infringements occurring in more than one country. In these situations, does Article 5(2) require the court to apply its own law, or may it apply

⁴¹⁸ Eugen Ulmer, *Intellectual Property Rights and the Conflict of Laws: a study carried out for the Commission of the European Communities, Directorate-General for Internal Market and Industrial Affairs* (Kluwer 1978) 10. Ulmer is not alone in interpreting Article 5(2) as meaning the *lex loci delicti*. See for example, Henri Desbois, André Françon and André Kerever, *Les conventions internationales du droit d'auteur et des droits voisins* (Daloz 1976) paras 135-9; André Lucas and Henri-Jacques Lucas, *Traité de la propriété littéraire et artistique* (2nd edn, Litec 2001) paras 1088-90.

⁴¹⁹ Eugen Ulmer, *Intellectual Property Rights and the Conflict of Laws: a study carried out for the Commission of the European Communities, Directorate-General for Internal Market and Industrial Affairs* (Kluwer 1978) 10.

⁴²⁰ *Ibid* 10 et seq.

⁴²¹ Sam Ricketson and Jane Ginsburg, *International Copyright & Neighbouring Rights - The Berne Convention and Beyond*, vol I (2nd edn, OUP 2006) 320.

the law of the country (or countries) where the infringement is alleged to have taken place (*lex loci delicti*)? Desbois et al argue that it would be illogical to insist on the *lex fori*, as it is the law of the country where the infringing act occurred which should be taken into account.⁴²²

Fawcett and Torremans argue that Article 5(2) points towards the law of the protecting country (*lex loci protectionis*). This law of the protecting country is the law of the country in which the work is being used, in which the exploitation of the work takes place.⁴²³ In their view, this interpretation follows from the logic of the Convention and the fact that Article 5 is actually determining the level of protection for those works that had previously qualified for protection under the Convention.⁴²⁴

Fawcett and Torremans give short shrift to the alternative minority interpretation (espoused by Koumantos) that the law of the protecting country refers to the country where the author is involved in legal proceedings⁴²⁵ and the suggested link with the law of the forum.⁴²⁶ They justify their rejection of the minority interpretation by pointing to

⁴²² Henri Desbois, André Françon and André Kerever, *Les Conventions internationales du droit d'auteur et des droits voisins* (Dalloz 1976) 153.

⁴²³ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) para 12.24. In their argumentation they cite Eugen Ulmer, *Intellectual Property Rights and the Conflict of Laws: a study carried out for the Commission of the European Communities, Directorate-General for Internal Market and Industrial Affairs* (Kluwer 1978) 11 ('the law of the country in which the work is being used') and Jane C Ginsburg, 'L'exploitation internationale de l'oeuvre audiovisuelle: France/États Unis' (1994) 4 *La Semaine Juridique* 49, Doctrine 3734 ('the law of the country in which the exploitation of the work takes place').

⁴²⁴ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) para 12.24.

⁴²⁵ Georges Koumantos, 'Sur le droit international privé du droit d'auteur' (1979) *Il Diritto di Autore* 616, 635 et seq; Geroges Koumantos, 'Privat International Law and the Berne Convention' (1988) 24 *Copyright* 415, 426.

⁴²⁶ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) para 12.25; citing Hakim Haouideg, 'Droit d'auteur et droit international privé en Belgique' (2006) 207 *RIDA* 98, 131; Sam Ricketson and Jane Ginsburg, *International Copyright & Neighbouring Rights - The Berne Convention and Beyond*, vol II (2nd edn, OUP 2006) 1299; Yves Gaubiac, 'La Convention de Berne, encore méconnue: commentaire de la decision TGI Paris, 3e ch., sect. B, 20 mai 2008, Sté des arts

the fact that in many circumstances, there will not even be proceedings, and also in those circumstances the parties may need to know which law is applicable, for example in the context of contractual negotiations.⁴²⁷

The idea that the law of the protecting country could be seen as an application of the law of the place where the tort was committed is also dismissed by Fawcett and Torremans as Article 5(2) is not primarily concerned with infringement⁴²⁸ but rather with any form of exploitation or use of the copyright work. They highlight the anomalous situation that has arisen in respect of the French Cour de Cassation in recent years. That court has set itself apart from other European jurisdictions by applying the law of the place where the tort was committed. The Cour de Cassation's distinctive approach likely derives from the fact that it does not see a choice of law rule in Article 5(2), Berne Convention, and, in the absence of a specific rule, IPR infringement is seen as a kind of a tort. That then brings in the law of the place where the tort was committed approach. Fawcett and Torremans level further criticism at the French court's focus on the act giving rise to the damage rather than the place where the damage occurs. They argue that this focus conflicts with the Rome II Regulation's approach⁴²⁹ but it also creates the risk of deliberate delocalisation of servers etc. to copyright havens.

Professors Geller and Ginsburg take a pragmatic view of the wording in Article 5(2). Geller suggests that the material part of the provision implies the application of the law

visuels et de l'image fixe [SAIF] c/SARL Google France, Sté Google Inc' (2008) 11 Communication Commerce Electronique 12, 14; and Alexandre Cruquenaire, 'La loi applicable au droit d'auteur: état de la question et perspectives' (2000) 3 Auteurs & Média 210, 212.

⁴²⁷ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011) para 12.25.

⁴²⁸ Their argument that the primary concern is not infringement conflicts directly with Ricketson and Ginsburg's contention that the application of Article 5(2) is limited to actual infringement proceedings which are brought to enforce rights protected under the Convention. Sam Ricketson and Jane Ginsburg, *International Copyright & Neighbouring Rights - The Berne Convention and Beyond*, vol II (2nd edn, OUP 2006) 1299.

⁴²⁹ See also CMV Clarkson and Jonathan Hill, *The Conflict of Laws* (4th edn, OUP 2011) 265 where they state that the general rule under Rome II is that the law applicable to a tortious obligation is 'the law of the country in which the damage occurs' (Article 4(1), Rome II).

effective where remedies take effect.⁴³⁰ Citing the preamble to the Berne Convention, which contains as one of its goals, the protection of authors' rights 'in as effective and uniform a manner as possible', Geller argues that the Convention suggests a principle of preference - apply the law that most effectively protects the work at issue.⁴³¹ Ginsburg has a similar contention. She suggests that the term may mean the forum country when that is the country from which the infringement originated, and which is best placed to accord an effective international remedy.⁴³²

Fawcett and Torremans' contention that the primary concern in the context of Article 5(2) is the form of exploitation or use of the copyright work, rather than infringement, seems to fly in the face of a literal interpretation of some of the words/phrases used in Article 5 (2), e.g. 'extent of protection', 'means of redress' ... 'to protect his rights' and 'where protection is claimed.'

The reference in Article 5(2) to 'the laws of the country where protection is claimed' seems to point to the *lex fori*, assuming that the phrase 'where protection is claimed' implies the initiation of legal proceedings by the copyright holder. As the claimant will most likely issue proceedings in the country where his copyright has been infringed (or most significantly infringed), then the *lex fori* is the likely outcome. While the *lex fori* may produce the most effective international remedy, it is far from certain that it coincides with the country from which the infringement originates (as per Ginsburg's assertion). The claimant copyright holder may have strategically focused his litigation on a country where pronounced secondary infringement (of his protected works) occurred. But such secondary infringement may relate to infringing material which originated from a different country.

⁴³⁰ Paul Edward Geller, 'Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked World' (1996) 20 Colum VLA JLA 571, 595.

⁴³¹ Ibid.

⁴³² Jane C Ginsburg, 'Comment, Extraterritoriality and Multiterritoriality in Copyright Infringement' (1997) 37 Va J Int'l L 587, 600.

5.4 The Rule of Origin versus the Rule of Reception

Having dealt with Rome II and the Berne Convention, I shall now turn to individual choice of law rules which have been formulated for the copyright and ICT sectors. In this regard, I shall treat the rule of origin⁴³³ and its various manifestations (e.g. Article 1(2)(b) of the SatCab Directive and Article 3(3) of the European Convention relating to questions on Copyright Law and Neighbouring Rights 1994), the advantages and disadvantages associated with the country of origin rule, and the law of the country of reception rule.

The rule of origin has had a relatively chequered history in copyright circles. And, while its popularity has waxed and waned over the past fifteen years or so, it may have become resurgent once again. Evidence for this is contained in the European Broadcasting Union's document, 'Modern copyright for digital media. Legal analysis and EBU proposals' published in March 2010.⁴³⁴ In this set of proposals, the EBU suggests that the solution adopted for EU-wide licensing for satellite broadcasting should be extended to communication to the public of audio and audiovisual media services via all electronic communications networks, including online.⁴³⁵

The rule of origin was initially incorporated into the EU's SatCab Directive.⁴³⁶ It was adopted again in both the European Convention relating to questions on Copyright Law and Neighbouring Rights 1994 and the European Commission's Green Paper of 27 July 1995 on Copyright and Related Rights in the Information Society. However, by

⁴³³ For an analysis of the rule of origin in the context of the E-Commerce Directive, see Julia Hörnle, 'The UK perspective on the country of origin rule in the E-Commerce Directive – A rule of administrative law applicable to private law disputes?' (2004) 12 IJLIT 333-363.

⁴³⁴ Stephen Edwards, Pascal Kamina and Karl-Nikolaus Pfeifer, 'Modern copyright for digital media. Legal analysis and EBU proposals' (EBU, March 2012) <http://www.ebu.ch/registration/policy2010/images/EBU%20Copyright%20WHITE%20Paper_EN_FINAL.pdf> accessed 2 July 2012.

⁴³⁵ Ibid 34.

⁴³⁶ Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15.

November 1996, when the European Commission issued its Communication on Copyright and Related Rights in the Information Society⁴³⁷ it was clear that the Commission had started to reconsider its view on the rule of origin. This new caution towards the rule of origin was linked to the Green Paper's consultation process when strong doubts emerged about transposing the approach of the SatCab Directive to the internet context. Two factors gave rise to the doubts. First, it may be difficult to identify a single point of origin of the transmission, and secondly, the point of origin could be in a country which denies any effective protection.⁴³⁸

5.4.1 The Satellite and Cable Directive

Under the SatCab Directive, there exists a workable mechanism for rights clearance with respect to a cross-border broadcast in the event of communication to the public by satellite of broadcasts originating in an EU Member State. This mechanism stipulates that any licensing of rights in the case of satellite communication is governed *solely* by the law of the Member State in which the communication of the same programme-carrying signal originates. In effect, it authorises the implementation of a 'one-stop-shop' for rights acquisition, since satellite communication rights may only be cleared in the country of origin.⁴³⁹

⁴³⁷ Commission, 'Follow-up to the Green Paper on Copyright and Related Rights in the Information Society' COM (1996) 568 final.

⁴³⁸ Ibid 23 et seq, fn 35; Jane C Ginsburg, 'Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks' (WIPO Forum on Private International Law and Intellectual Property, GCPIC/2, 1998) 42, fn 136.

⁴³⁹ A similar type situation prevails in respect of audiovisual services. Under Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 amending Council Directive 89/552/EC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities [2007] OJ L332/27, art 1.3. (also referred to as the Audiovisual Media Services without Frontiers Directive) the former Article 2 of the Television Without Frontiers Directive is replaced with a new provision which provides that each Member State shall ensure that all audiovisual media services transmitted by media service providers under its jurisdiction comply with the rules of the system of law applicable to audiovisual media services intended for the public in that Member State.

The 1993 Directive does not have an obvious nexus with the internet,⁴⁴⁰ but it regulates an area of transnational communication and it covers communication channels through which significant digital copyright material passes. It is clear that its scope of application extends over transborder transmissions of digitised material, analogous to the workings and contents of internet transmissions. The Directive's relevance is increased by the fact that the physical infrastructure of the internet comprises satellite and cable components, for example, VSAT systems (internet over satellite) and fibre optic cables (submarine cables).

While, *sensu stricto*, the rule of origin in the SatCab Directive is not a rule of private international law,⁴⁴¹ it has a strong influence on choice of law matters.

By defining broadcasting in this way, the Directive ensures that only the laws of the country from where the broadcast originates will govern any copyright infringement relating to that broadcast. The approach in the Directive is to attach more significance to the original transmission of the signal than to its reception. The German 'Felsberg' ruling⁴⁴² demonstrates how the provision is applied. There, German law was held to apply to a broadcast made from Germany, but addressed to a French public and possibly received by some Germans, on the basis that 'control' of the broadcast was exercised at the point of broadcasting in Germany.

⁴⁴⁰ Geller argues that there is little analogy between broadcasts or even cablecasts and internet transmissions. In broadcasts/cablecasts, one broadcaster or cablecaster alone decides whether to communicate a work from any one country to multiple points all at once. In internet transmissions, telecommunication is interactively effected among multiple and possibly mobile points in cyberspace. In this fluid situation, the courts have not yet consistently localised possibly infringing transactions prior to choosing applicable laws. Paul Edward Geller, 'Conflicts of Laws in Copyright Cases: Infringement and Ownership Issues' (2004) 51 J Copyright Soc'y USA 315, 351.

⁴⁴¹ Though note the views of Dinwoodie, Dreyfuss and Kur that the rule in the SatCab Directive can be conceptualised as a harmonised choice of law rule, dictating in which State the transborder act will be deemed to occur. Graeme B Dinwoodie, Rochelle C Dreyfuss and Annette Kur, 'The Law Applicable to Secondary Liability in Intellectual Property Cases' (2010) 42 NYU Journal of International Law and Politics 201, 225, fn 59.

⁴⁴² BGH GRUR 2003, 328 ('Felsberg Transmitter' decision).

5.4.1.1 The Definitional Rule

The Directive, in effect, ‘localises’⁴⁴³ the act of communication, not in the receiving country/countries but ‘solely in the Member State where, under the control and responsibility of the broadcasting organisation, the programme-carrying signals are introduced into an uninterrupted chain of communication’.⁴⁴⁴ If one were to analogise and apply the country of origin rule to digital transmissions, the initiating act should be deemed to take place at the location of the server that hosts the infringing website. However, where the relevant server is located in a copyright haven, then the initiating act should be deemed to take place in the country of the defendant’s residence or principal place of business. Ginsburg argues that where both of the aforementioned places are copyright havens, then the ‘initiating act’ point of attachment should not apply.⁴⁴⁵

5.4.1.2 Third Countries Satellite Communications

The directive also covers the complicated situation where the act of communication by satellite occurs in a third country which does not provide the required minimum level of protection set out in Chapter II of the Directive. Generally, the copyright-triggering act occurs in the physical place of uplink.⁴⁴⁶

But if this place is located outside the EU and it does not provide for adequate protection and the uplinking organisation has its headquarters in the EU, then the

⁴⁴³ Ginsburg actually uses the term ‘localizes’ when analysing the effect of Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15, art 1.2.(b). Jane C Ginsburg, ‘Berne Without Borders: Geographic Indiscretion and Digital Communications’ (2002) 2 IPQ 111, 116, fn 20.

⁴⁴⁴ Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15, art 1.2.(b).

⁴⁴⁵ Jane C Ginsburg, ‘Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks’ (WIPO Forum on Private International Law and Intellectual Property, GCPIC/2, 1998) 44.

⁴⁴⁶ Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15, art 1.2.(b).

Satellite Directive prefers the intellectual to the physical location of the place of the uplink: the Directive provides that the location of the headquarters will trump offshore siting of the physical equipment of uplinking.⁴⁴⁷

5.4.1.3 *Footprint Countries*

Interestingly, it seems that in applying the *lex emissionis*, account may also be taken of the laws of footprint countries. Footprint countries are those in which the broadcast is received. Most broadcasters encrypt their signals to avoid unauthorised reception by the public and also to limit their potential and thereby restrict the scope of the broadcasting rights that they have to acquire in the works involved. For these signals to be decrypted, the user has to possess a decoder and in most cases, a smart card as well. Thus the criterion for determining whether a specific country should be considered as a footprint country must be whether the decoder equipment together with the smart card are lawfully available to the public or section of the public of the country in question.⁴⁴⁸

⁴⁴⁷ Jane C Ginsburg, 'The Cyberian Captivity of Copyright: Territoriality and Authors' Rights in a Networked World' (1999) 15 Santa Clara Comp & Tech LJ 347, 359. The act of communication to the public is 'deemed to have occurred in the Member State in which the broadcasting organization has its principal establishment'. Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15, art 1.2.(d)(ii).

⁴⁴⁸ On 4 October 2011, the CJEU handed down its ruling in *Joined Cases C-403/08 and C-249/08 Football Association Premier League v QC Leisure and Others; and Karen Murphy v Media Protection Services Ltd* [2011] ECR I-9083. This case concerned foreign decoder cards. In short, the Court of Justice held that a licence system for the broadcasting of football matches based on absolute territorial exclusivity and which prohibited TV viewers from watching broadcasts with a decoder card from another Member State was contrary to EU Law. Viewed from a Competition Law perspective, Article 101 TFEU was infringed where exclusive licence agreements between an IP holder and a broadcaster obliged the latter not to supply decoding devices with a view to their use outside the exclusive licence territory. The case also involved important points under Article 56 TFEU (Freedom to Provide Services). In the final analysis, the CJEU ruled that a restriction which offended Article 56 TFEU could not be justified in light of the objective of protecting IPRs. In concluding the fundamental freedoms section of its judgment, the CJEU referred to the development of EU Law, in particular the adoption of the Television without Frontiers Directive and the Satellite Broadcasting Directive, which are intended to ensure the

In two decisions, one French, the other Austrian, and both relating to traditional terrestrial broadcasting of copyright-protected programmes, it was held that broadcasters must comply with the laws of the footprint countries either because damage occurred there (French decision) or because they were intended to be received by the audience of that country (Austrian decision).⁴⁴⁹ The broadcasters, as defendants, had argued that the notion of copyright in broadcasting could only be applied to the act of emission, and that consequently the only applicable copyright law was the one enjoyed by right owners.

5.5 The European Commission's 1995 Green Paper on Copyright⁴⁵⁰

The relative popularity of the rule of origin is further demonstrated by the fact that it was contained in the European Commission's 1995 Green Paper on Copyright.⁴⁵¹ The Commission published its Green Paper in July 1995, almost a year after the US published its own Green Paper. The EU Green Paper contains a short section entitled 'Applicable Law'. It describes how community law affects questions relating to the applicable law and refers to the SatCab Directive. In recognising the importance of determining which law is to apply in cross-border situations, it recommends the use of

transition from national markets to a single programme production and distribution market. See generally Mark Hyland, 'The Football Association Premier League ruling – the Bosman of exclusive broadcasting rights?' (2012) 17 Comms L 7-13.

⁴⁴⁹ Philippe Kern, 'The EC "Common Position" on Copyright Applicable to Satellite and Cable' (1993) 8 EIPR 276, 279 et seq. The cases are: *Radio Périphériques v SNEP* (2009) 144 RIDA 215, Cour d'Appel de Paris; Oberster Gerichtshof 28.5.1991, 4 Ob 19/91; OGH ÖBl 1991, 181; GRUR Int 1991, 920 ('Tele Uno III' decision). In 'Tele Uno III', it was held that in addition to the law of the country of emission, the copyright laws of all those countries situated at least to a considerable extent within the regular reception scope of such broadcasts must be applied. Paul Edward Geller, 'Conflicts of Laws in Copyright Cases: Infringement and Ownership Issues' (2004) 51 J Copyright Soc'y USA 315, 350, fn 160.

⁴⁵⁰ Commission, 'Green Paper: Copyright and related rights in the information society' COM (1995) 382.

⁴⁵¹ *Ibid* and 38-43. This contrasts with the 2008 Commission, 'Green Paper: Copyright in the Knowledge Economy' COM (2008) 466/3 which does not refer to the rule of origin or to the applicable law for that matter.

the country of origin rule.⁴⁵² It acknowledges that a community rule on the applicable law seems to be indispensable and that such a rule should be along the lines of that which is contained in the SatCab Directive.⁴⁵³

However, in applying this rule, judges would be obliged to apply the law and regulations of countries with which they are not entirely familiar, a principle thought to have been long rejected in international copyright.⁴⁵⁴ In addition, the apparent simplicity of the rule belies real difficulties in determining the origin of a work on the internet. An example of such a difficulty is the use of anonymous remailers where indicators of a work's source are removed.⁴⁵⁵

Interestingly, the Commission's views had changed considerably by November 1996 when it issued its Communication on Copyright and Related Rights in the Information

⁴⁵² Schönning analyses the differences between a country of origin approach and a country of destination approach as regards determining the applicable law in online copyright scenarios. Where a country of destination approach is used, the law of the country where the transmission is received will apply. Schönning acknowledges that 'there are arguments for both options and that there is as yet, no international solution.' But he believes that the country of reception rule is preferable from the copyright owner's perspective: 'For authors, it would without doubt be preferable to choose the country of reception. Using the law of the country of reception, it is possible to evade so-called copyright havens, ie the possibility of transmitting legally unauthorized material from countries with no protection of copyright or authors' rights'. Peter Schönning, 'Licensing Authors' Rights on the Internet' (2000) 31 IIC 967, 973 et seq. Schönning's preference for the country of reception rule may be somewhat misguided as it is always open to the infringer to target/send the infringing material to recipients who are based in, or deliberately base themselves in copyright havens knowing full well that the illegal transmission will be covered by the law of the destination country.

⁴⁵³ Commission, 'Green Paper: Copyright and related rights in the information society' COM (1995) 382, 42.

⁴⁵⁴ Stephen M Stewart, *International Copyright and Neighbouring Rights* (2nd edn, Butterworths 1989) 185: 'The history of copyright reflects the development of technology'. Stewart analyses the failure of the Montevideo Convention of 1889 and the avoidance of this 'mistake' by the Berne Convention.

⁴⁵⁵ Daniel Akst, 'Postcard from Cyberspace: The Cutting Edge, The Helsinki Incident and the Right to Anonymity' *LA Times* (Los Angeles, 22 February 1995) D1.

Society.⁴⁵⁶ While the Commission acknowledged that new means of communication (internet/new digital satellites) would increase the relevance of applicable law issues, it made it clear that during the Green Paper's consultation process, strong doubts had emerged about transplanting the approach of the SatCab Directive to the internet context. Two factors gave rise to the doubts. First, it may be difficult to identify a single point of origin of the transmission and, (cross ref defamation analogue) secondly, the point of origin could be in a country which denies any effective protection.⁴⁵⁷ This latter factor also arose in relation to the Council of Europe Convention on Copyright and proposed limitations being placed on its rule of origin.

5.6 Advantages Associated with the Country of Origin Rule

Proponents of the country of origin theory point to its simplicity.⁴⁵⁸ Provided the rule incorporates a workable definition of the place from where a communication to the public originates, a country of origin rule offers greater predictability than choice of law rules linked to the place of reception, or, more ambiguous still, to the economic impact of an act of exploitation.⁴⁵⁹ From the plaintiff copyright holder's perspective, the

⁴⁵⁶ Commission, 'Follow-up to the Green Paper on Copyright and Related Rights in the Information Society' COM (1996) 568 final.

⁴⁵⁷ Ibid 23 et seq and fn 35; Jane C Ginsburg, 'Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks' (WIPO Forum on Private International Law and Intellectual Property, GCPIC/2, 1998) 42, fn 136.

⁴⁵⁸ There is no doubt but that a choice of law rule that designates the law of a single country to govern the ensemble of internet copyright transactions would considerably simplify the legal landscape and possibly promote internet commerce. Jane C Ginsburg, 'Copyright Use and Excuse on the Internet' (2000) 24 Colum VLA JLA 1, 44.

⁴⁵⁹ Laurence GC Kaplan and Joseph R Bankoff, 'Of Satellites and Copyright: Problems of Overspill and Choice of Law' (1993) 7 Emory Int'l L Rev 727, 741. The law of the country of origin was applied by the Second Circuit in *Itar-Tass Russian News Agency v Russian Kurier, Inc*, 153 F 3d 82 (2d Cir 1998) despite the fact that the court labelled it the law of the country with 'the most significant relationship' to the work. Paul Torremans, 'Private International Law Aspects of IP – Internet Disputes' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet: a Framework for Electronic Commerce* (2nd edn, Hart Publishing 2000) 244, fn 98.

application of the country of reception⁴⁶⁰ principle is unsatisfactory since it would result in the application of a different copyright law in each set of national proceedings, where the infringing material is received in all twenty-eight EU Member States. It is not an exaggeration to state that copyright laws differ significantly as between the twenty-eight EU Member States. Nor is the hypothesis that the infringing material be received in every EU Member State an unrealistic one. After all, the internet is accessible from virtually every country in the world.

It would seem that a combination of the country of origin and the country of reception rules would not assist the conflicts lawyer since it would only increase legal uncertainty. It would, in effect, lead to the application of more than one law in most cases and this would destroy the desired objective of creating a situation where only *one* law is deemed to be the applicable law.⁴⁶¹

⁴⁶⁰ Torremans refers to this country as the ‘country of receipt’. Paul Torremans, ‘Private International Law Aspects of IP – Internet Disputes’ in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet: a Framework for Electronic Commerce* (2nd edn, Hart Publishing 2000) 245.

⁴⁶¹ Torremans puts forward alternative points of attachment. They are, as follows:

1. The normal rule should be that any infringement issue is governed by the law of the country in which the server that hosts the allegedly infringing content is located.
2. If the law that is applicable under the normal rule does not meet the minimum standards that have been laid down in the Berne Convention, the TRIPs Agreement and the WCT, that law should be replaced by the law of the country in which the operator of the website that contains the allegedly infringing material has its residence or its principal place of business.
3. If the law that applies under 2 also does not meet the minimum standards that have been laid down in the Berne Convention, the TRIPs Agreement and the WCT, the law of the forum will be the applicable law if the law of the forum meets the minimum standards that have been laid down in the Berne Convention, the TRIPs Agreement and the WCT.

Paul Torremans, ‘Private International Law Aspects of IP – Internet Disputes’ in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet: a Framework for Electronic Commerce* (2nd edn, Hart Publishing 2000) 245. This approach is also suggested by Jane C Ginsburg, ‘Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks’ (WIPO Forum on Private International Law and Intellectual Property, GCPIC/2, 1998) 44 et seq.

But what if the copyright material is downloaded in country Y (having been sent from country X), copied and modified without the owner's authorisation, and then uploaded with the specific intention of dissemination over the internet. Which law would apply to this infringement? The law of the country from which the material was originally requested (X), or, the law of the country where the infringing material was created and then transmitted online? I would argue that the relevant law for the act of transmitting infringing material is the new country of transmission (i.e. country Y) as the illegal copying/modification in country Y constitutes a fresh tort.

5.7 Disadvantages Associated with the Country of Origin Rule

The rule is not without its critics. Some argue that the rule of origin facilitates the extraterritorial application of foreign copyright law. The copyright law of the state of origin will apply no matter where the copyright material is sent on the internet. Another difficulty may arise in determining the exact point from where the infringing material originated. Though, this particular problem may be soluble through the application of geolocation technology.

One considerable disadvantage of applying the country of origin rule is that it results in different copyright laws governing works in the same country. This becomes problematical for people who exploit these rights since, in effect, they have to know the country of origin of each work and are obliged to have comprehensive knowledge of a potentially large number of national copyright regimes. Is this expectation realistic?

Where the country of origin rule is applied, the rights of copyright holders may be undermined when individual infringers and suspect ISPs deliberately relocate to jurisdictions with weak copyright laws, safe in the knowledge that their illegal online transmissions will be subject to the local law.⁴⁶² This application of the local law (the

⁴⁶² Jane C Ginsburg, 'Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks' (WIPO Forum on Private International Law and Intellectual Property, GCPIC/2, 1998) 42; Jane C Ginsburg, 'The Cyberian Captivity of Copyright: Territoriality and Authors' Rights in a Networked World' (1999) 15 Santa Clara Comp & Tech LJ 347, 359. In this article, Ginsburg analyses the issue of the point of departure. Is it the place where the server is located, or the place where the website operator has its residence or headquarters? Under the SatCab Directive, the copyright-engaging act occurs in the physical place of uplink. A point of origin approach

rule of origin) is tantamount to localising an infringing act in the country of transmission (or source country). One runs the risk however of unreliably ‘exporting’ that country’s purely local copyright policies into other countries whose markets and audiences are impacted by the transmission.⁴⁶³ Suppose, for example, that country A provides less protection than country B in a given case: applying A’s laws to outgoing transactions that target B’s market would impose standards of protection on B lower than B’s legislature intended for its home market in that case, just as applying B’s law to outgoing transactions that target A’s market would have the opposite effect in A.⁴⁶⁴ To safeguard against the relocation of intellectual property infringers to underprotective ‘copyright havens’, the EU and other copyright-producing States have resisted the point of origin approach for internet transmissions involving copyrighted material.⁴⁶⁵

may also spark a ‘race to the bottom’ among copyright pirates as they gravitate to States with substandard copyright laws. In addition, this approach can have the effect of extruding the country of origin’s copyright policy choices to the detriment of copyright policies in the other countries of receipt. Jane C Ginsburg, ‘Copyright Use and Excuse on the Internet’ (2000) 24 Colum VLA JLA 1, 44. In his analysis of localization issues in the domain of online copyright, Geller distinguishes between ‘initiating acts’ and ‘consummating acts’. He propounds the following rule of thumb: ‘*Localize any allegedly infringing act in a given country only if the transaction including that act is incoming relative to that country.*’ (emphasis added). Paul Edward Geller, ‘Conflicts of Laws in Copyright Cases: Infringement and Ownership Issues’ (2004) 51 J Copyright Soc’y USA 315, 339.

⁴⁶³ Paul Edward Geller, ‘Conflicts of Laws in Copyright Cases: Infringement and Ownership Issues’ (2004) 51 J Copyright Soc’y USA 315, 339.

⁴⁶⁴ This brings into play the distinction between incoming and outgoing transactions relative to any given country. Generally speaking, a transaction is incoming relative to a given country if it tends to impact the market or audience in that country, and it is outgoing if, starting in that country, it tends to impact the market or audience in another country. Geller argues that localization of any infringement in a particular country should only occur if the transaction including that act is incoming relative to the country in question. See Paul Edward Geller, ‘Conflicts of Laws in Copyright Cases: Infringement and Ownership Issues’ (2004) 51 J Copyright Soc’y USA 315, 338 et seq.

⁴⁶⁵ Jane C Ginsburg, ‘Berne Without Borders: Geographic Indiscretion and Digital Communications’ (2002) 2 IPQ 111, 116. It is worth noting that Article 3(1) of the E-Commerce Directive contains a rule of origin. However, a derogation from the effects of Article 3(1) has been granted to copyright, neighbouring rights and industrial property rights. See the Annex (‘Derogations from Article 3’) to the Directive where the following is

While the country of origin rule could undoubtedly be exploited by copyright infringers, it may also serve the copyright owner's purposes and guarantee a certain level of copyright protection. When used constructively by the copyright owner, it gives rise to an author-centric approach to copyright protection. The author can choose a safe jurisdiction (i.e. a jurisdiction applying high levels of intellectual property protection) from which to disseminate copyright works over the internet. In doing so, the copyright holder can publish on the internet, safe in the knowledge that the copyright law of that jurisdiction will apply, no matter where in the world he sends the material.

5.8 Points of Attachment

A difficulty may arise with the identification of a meaningful point of attachment. If a country had a particularly significant relationship to the creation or communication of the work, its law could govern all issues from protection through to infringement. And, given the effects of digital communications, perhaps the only fixed point in the equation is the author. For example, the country of the author's residence (at the time of the work's first public disclosure) could be deemed the country of origin. The law of the author's residence could then be deemed the governing law when adjudicating claims of copyright ownership and multi-territorial infringements.⁴⁶⁶ A possible objection to this proposal is that it may promote a peculiar variant of what American conflicts scholars call the 'race to the bottom'.⁴⁶⁷ The variant here would be the opposite: authors would

stated: 'As provided for in Article 3(3), Article 3(1) and (2) do not apply to: – copyright, neighbouring rights, rights referred to in Directive 87/54/EEC(1) and Directive 96/9/EC(2) as well as industrial property rights'.

⁴⁶⁶ Ginsburg argues that the author's residence may be a more convincing criterion since the internet drastically compromises the place of first publication point of attachment. It also extravagantly multiplies the countries of exploitation/infringement. Jane C Ginsburg, 'Berne Without Borders: Geographic Indiscretion and Digital Communications' (2002) 2 IPQ 111, 121.

⁴⁶⁷ The 'race to the bottom' connotes that persons subject to the law's regulation will seek the most forgiving jurisdiction possible, such as the Cayman Islands in financial matters. The phenomenon arises too in the area of tax competition, where European tax havens such as the islands of Guernsey, Jersey and the Isle of Man lead the way by offering zero tax rates to both resident and non-resident companies. Bruno Gurtner and John Christensen, 'Beyond Bretton Woods: The Transnational Economy in Search of New Institutions - The Race to the Bottom: Incentives for New Investment?' (*tax justice network*, 15-17 October 2008)

flock to the jurisdiction offering the most author-favourable norms. Countries might actually vie with one another to attract authors to their shores. A possible example is France and its author-friendly copyright laws which have attracted many American writers.⁴⁶⁸

If one views international copyright as simply a collection of national markets, each of which is subject to local definition, then the countries with the most significant relationship to the harm are the countries whose markets the unauthorised digital communication disrupts. This view leads to the application of the laws of the countries of receipt, possibly tempered by a presumption as to the similarity of their content with the substantive copyright law of the forum.

If, by contrast, one considers that the country from which the infringement originated, either physically or intellectually, as the country with the most significant relationship to the ensuing harm, then one is likely to favour application of the law of the server or of the initiator's residence/principal place of business, at least so long as this country is not a 'copyright haven'.

As regards online copyright infringements, perhaps the best approach is one which combines certain aspects of the SatCab Directive with alternative points of attachment, such as:

1. The law applicable to the entirety of a defendant's alleged internet infringement is the law of the country in which the server that hosts the alleged infringing content is located, so long as this country's domestic copyright law is consistent with Berne Convention and WIPO Copyright Treaty norms.
2. If the law of the country identified in paragraph 1 is inadequate, then the law applicable to the entirety of the defendant's alleged internet infringement is the

<http://www.taxjustice.net/cms/upload/pdf/Bruno-John_0810_Tax_Comp.pdf> accessed 2 July 2012.

⁴⁶⁸ Jane C Ginsburg, 'Berne Without Borders: Geographic Indiscretion and Digital Communications' (2002) 2 IPQ 111, 120. In the same article (also at page 120), Ginsburg goes on to point out that the proposal covering the law of the author's residence, brings us full-circle to the nineteenth century debate (at least in France) over whether the State of the Author, or the State of the first publication, or the State where the alleged infringement occurs is the relevant point of attachment for international copyright.

law of the country in which the operator of the website on which the allegedly infringing content is found has its residence or principal place of business, so long as this country's domestic copyright law is consistent with Berne Convention and WIPO Copyright Treaty norms.

3. If the law of the country identified in paragraphs 1 and 2 is inadequate, then the law applicable to the entirety of the defendant's alleged internet infringement is the law of the forum, so long as the forum is a member of the Berne Union or WTO (or WIPO Copyright Treaty), but the parties may demonstrate that, for particular countries in which alleged infringements occurred, the domestic law is either more or less protective than the copyright or related rights law of the forum.

As can be seen from the above three suggested solutions, the principal point of attachment for determining the choice of law is the site of the defendant's server or his residence/place of business. Where neither is adequate, the law of the forum will prevail provided it meets with minimum international standards.

5.9 An Alternative – The Law of the Country of Reception

An alternative to the rule of origin is to apply the law of the country of reception. However, this approach may be problematical since it is technically feasible for there to be one or more points of reception in every one of the twenty-eight EU Member States. Were this to occur, each Member State would constitute a country of reception. Consequently, each court in a country of reception would apply its own law.⁴⁶⁹ Another

⁴⁶⁹ A country of reception rule would become even more difficult to apply if its geographic scope of application were ever to extend beyond the EU. Since most countries in the world have internet facilities (albeit with wide divergences between developed and developing countries' penetration rates), it is conceivable that material posted on the Internet could be simultaneously received in countless countries. If the internet transmission featured copyright-infringing material, the governing law would be that of the place where the material was finally received by an internet user. It would seem that if separate sets of legal proceedings were instituted by the copyright owner, each set would be governed by a different law, depending on where the infringing material was finally received. This would be an unsatisfactory situation from the copyright holder's perspective since, while his rights would have been infringed, he would have no control over which law would be the applicable law in the proceedings. Where this rule applies, the chances of the copyright

line of thinking holds that this approach may involve the cumbersome consequence of the competent court applying the laws of every country in the world where the internet can be received.⁴⁷⁰ This raises the issue of whether a national forum would have jurisdiction to hear the full geographical scope of copyright infringement claims against a foreign defendant, who has made a work available in every country of the world, but who neither resides in, nor has made the work available from the forum in question (for example, the defendant sends the infringing work to a webpage hosted by a server in the country where the seised court is situated).

The application by each court (in a country of reception) of its own law would certainly prove convenient for the individual courts. However, it may not be so convenient for the plaintiff since what begins as a single copyright infringement, transmitted via the internet, may develop into at least⁴⁷¹ twenty-eight separate sets of proceedings, with each court applying its own copyright law. Furthermore, EU copyright law has not been fully harmonised and the disparities between national copyright systems will increase further under Directive 2001/29/EC.⁴⁷² And, looking beyond the EU, let us take the following hypothetical case. Buster Keaton's silent film classic 'The General' is colourised by an online service without the permission of the copyright holder. It is

holder's own law constituting the governing law in proceedings would be very slim indeed. Jane C Ginsburg, 'Berne Without Borders: Geographic Indiscretion and Digital Communications' (2002) 2 IPQ 111, 116 et seq.

⁴⁷⁰ Jane C Ginsburg, 'The Cyberian Captivity of Copyright: Territoriality and Authors' Rights in a Networked World' (1999) 15 Santa Clara Comp & Tech LJ 347, 349 et seq, fn 4 at 350.

⁴⁷¹ The term 'at least' has been used since the infringing material may be downloaded by more than one person in the country of reception. In addition, certain Member States comprise more than one jurisdiction, e.g. the UK, whilst the complicated federal structure in Germany, Belgium and Austria may generate various sets of legal proceedings in the different federal regions within those particular Member States.

⁴⁷² Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10, art 5 contains exceptions and limitations to the reproduction right set out in Article 2 of the directive. In summary, Article 5 lists twenty cases where the Member States may provide for exceptions or limitations to the reproduction right. Generally, see the views of Thomas C Vinje, 'Should We Begin Digging Copyright's Grave?' (2000) 22 EIPR 551; and Bernt Hugenholtz, 'Why the Copyright Directive is Unimportant, and Possibly Invalid' [2000] EIPR 499, 500 et seq.

stored on a computerised database in the US and end-users are allowed to download the work on demand through a global network: end-users receive the work at their private terminals worldwide. However, while the work is in the public domain in the US, it is still protected by copyright in Germany and, though unprotected by economic rights in France, still protected by moral rights there. To the extent that these transactions are incoming relative to Germany and France, infringement could be localised there. But, in applying the rule of reception very different levels of copyright protection are provided.

Another risk associated with the application of a rule of reception is that it may cause a race to underprotective copyright havens in reverse. If such a rule were to prevail, copyright pirates would direct their infringing material to jurisdictions with lax intellectual property laws⁴⁷³ in the full knowledge that a weak copyright law will be applied by the judge in the court proceedings.

5.10 Conclusions

Despite the fact that the *lex loci protectionis* was not exactly the ‘universally acknowledged principle’ it was described as (in Recital (26) of Rome II), it is arguable that it produces a higher degree of legal certainty than the situation which prevailed pre-Rome II. However, the trade-off for that certainty is an increased regulatory burden for commercial parties, requiring more extensive investigation of national IPRs both when planning new cross-border business activity and, in the event of a dispute, prior to commencing or defending litigation. Adoption of the *lex loci protectionis* in Rome II may yet prove to be a stop-gap solution pending further consolidation of IPRs or the associated rules of PIL at a European or international level.⁴⁷⁴

⁴⁷³ According to ‘Imitation v Inspiration’ *The Economist* (US, 14 September 2002) 11: ‘Most of the world’s people live in countries which either do not have, or do not enforce, intellectual property rights.’ However, this situation will not prevail for much longer. TRIPS requires even the least-developed countries to have some minimum protection in place by 2006, though some of the world’s least developed countries have argued that they need till 2016 to implement certain forms of intellectual property protection e.g. the adoption and enforcement of patents on pharmaceuticals. All countries joining the World Trade Organisation (WTO) must also sign up to TRIPS (Trade-related aspects of intellectual-property rights).

⁴⁷⁴ Andrew Dickinson, *The Rome II Regulation – The Law Applicable to Non-Contractual Obligations* (1st edn, OUP 2008) 460.

The ambiguous wording of Article 5(2) Berne Convention has provoked considerable debate about its precise meaning and nature (i.e. is it a real choice of law rule? (van Eechoud)). Having examined the views of a large number of commentators I believe Article 5(2) points towards the *lex fori*, assuming that the phrase ‘where protection is claimed’ implies the initiation of legal proceedings by the copyright holder. If the place of the legal proceedings coincides with the place of infringement, then both *lex fori* and *lex loci delicti* will point to the same applicable law.

Ginsburg is also of the view that the term may mean the forum country provided that it is the country from which the infringement originated and it is best placed to accord an effective international remedy.⁴⁷⁵ I do not agree with Ginsburg’s two conditions, particularly the first, as in a large number of cases, there will be no obvious nexus/overlap between the forum country and the country from which the infringement originated. Instead, the claimant will have chosen to issue legal proceedings in the forum country for strategic reasons.

The cyclical nature of some of the applicable law principles is demonstrated by the re-emergence in March 2010 of the rule of origin in a set of EBU Proposals. The proposals recommended that the solution adopted for EU-wide licensing for satellite broadcasting, in short, a rule of origin, should be extended to communication to the public of audio and audiovisual media services via all electronic communications networks, including online.⁴⁷⁶

⁴⁷⁵ Jane C Ginsburg, ‘Comment, Extraterritoriality and Multiterritoriality in Copyright Infringement’ (1997) 37 Va J Int’l L 587, 600.

⁴⁷⁶ Stephen Edwards, Pascal Kamina and Karl-Nikolaus Pfeifer, ‘Modern copyright for digital media. Legal analysis and EBU proposals’ (*EBU*, March 2012) 34 <http://www.ebu.ch/registration/policy2010/images/EBU%20Copyright%20WHITE%20Paper_EN_FINAL.pdf> accessed 2 July 2012.

Chapter 6. Models and analogues for online copyright infringement, how compelling is the defamation analogue?

TABLE OF CONTENTS

6.1	The aim of this chapter	165
6.2	Push/Pull dichotomy	166
6.3	Copyright’s exclusive rights	168
6.4	The scope of my analysis in this chapter	169
6.5	Conceptual Models	171
6.6	A definition of defamation and how it evolves through the case-law	172
6.7	Online Defamation	173
6.8	Online Copyright Infringement	177
6.9	Points of connection/disconnection between online defamation and online infringement of the reproduction right.....	183
6.9.1	Points of Connection:	183
6.9.2	Points of Disconnection:.....	184
6.10	Communication to the Public.....	185
6.10.1	Dramatico Entertainment Limited v British Sky Broadcasting.....	186
6.10.2	EMI Records Limited v British Sky Broadcasting Limited	187
6.10.3	Football Association Premier League Limited v British Sky Broadcasting..	191
6.11	Points of connection/disconnection.....	192
6.12	Right of making available to the public: the views of various commentators	194
6.13	Possible application of the communication theory and the emission theory	194
6.14	Where the making available right takes place according to Sterling.....	195
6.15	European Commission’s Localisation Criteria for the Making Available Right	197
6.16	Criterion No. 1 - Location of the servers upon which the works are hosted (step 3)	197
6.17	Criterion No. 2 – Centre of activities of the uploader: establishment, domicile or habitual residence (no correspondence with the ‘step’ analysis) ...	198
6.17.1	The Advantage of using this criterion	199

6.17.2	Some problems arising from use of this criterion	200
6.18	Criterion No 3 – Where the material act of upload is initiated (Step 2) .	201
6.18.1	Some problems associated with this criterion	202
6.19	Points of connection/disconnection between Sterling and the European Commission Study on the making available right	202
6.19.1	Points of connection	202
6.19.2	Points of disconnection.....	203
6.20	Conclusions	203
6.20.1	Reproduction right versus Defamation	203
6.20.2	Online Communication to the public versus online defamation.....	204
6.20.3	The Making Available Right.....	205

6.1 The aim of this chapter

The aim of this chapter is to critically evaluate and compare the two online torts which form the backbone of my research, namely online copyright infringement (the case study) and the analogue - online defamation - and to determine how compelling (or not) the defamation analogue actually is. Copyright will be divided up into three of its constituent restricted rights, namely, the reproduction right, the communication to the public right and the making available right. As regards the defamation component, since libel is the permanent form of defamation, and is usually deemed by statute to occur by broadcasting and related forms of communication,⁴⁷⁷ I shall be focusing on this branch of defamation. At various points in the chapter, I shall highlight the points of connection (crossover points) and points of disconnection between the two torts.

Another important theme running through this evaluation is that of localisation of the relevant tort. As will become evident, jurisprudence has a key bearing on the criteria used for localisation. In terms of online defamation, I have drawn considerably from the Australian High Court ruling in the defamation case of *Dow Jones v Gutnick*.⁴⁷⁸ Despite its falling outside my primary jurisdictional focus, it remains a landmark judgment and is too important and influential to omit. Importantly, it is cited by Sterling as relevant to locating acts of online copyright infringement.⁴⁷⁹ As regards the right of communication

⁴⁷⁷ Perhaps surprisingly, the question whether internet communications amount to libel or slander appears to have attracted comparatively little attention in the case law. Communications from an internet site (such as a web page) would seem to come within Section 201(1)(b) of the Broadcasting Act 1990 [and hence constitute libel under s 166] (because they are sent by a telecommunications system for reception at two or more places). Richard Parkes, Alastair Mullis and Godwin Busuttill, *Gatley on Libel and Slander* (12th edn, Sweet & Maxwell 2013) 3.12 .

⁴⁷⁸ *Dow Jones v Gutnick* [2002] HCA 56.

⁴⁷⁹ JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 152, where Sterling states as follows:

While the Gutnick case concerned an action for defamation, it is thought that, in the context of infringement on the internet, it provides notable support for the proposition that, since liability for tort will arise at the place where the infringing act occurs or where the consequent damage arises, liability for infringement of copyright/author's right/related rights arises in the case of the internet, at the place where the infringing act occurs or where damage flows from the act. Transmission

to the public, the web-blocking case law under s. 97A CDPA 1988 (see 7.3.5.) has proven pivotal in establishing important criteria to determine whether a communication to the public can be localised in the UK or not. Later in this chapter (from para 6.10 onwards), I critically evaluate the criteria adopted by the English High Court to determine whether a communication to the public can be localised in the UK or not.

6.2 Push/Pull dichotomy

Before moving onto copyright's exclusive rights, I shall mention the push/pull dichotomy in information technology, outlined by Svantesson.⁴⁸⁰

Put briefly, pushed communications are synchronous (that is available only at a particular time) while pulled communications are asynchronous (i.e. available at the time of the consumers' choosing). To give some examples, World Wide Web communications are considered a form of pull technology while television, radio broadcasts and emails are considered a push technology. Push technology can also be amenable to user preference: an internet user may subscribe to, say, a news service, indicating in advance the topics on which he wishes to receive information.

The 'ecommerce technology' web site has this to say:

“Currently, one of the most fashionable technologies within the Internet is “Push” technology. Contrary to the “Pull” world of web pages where users request data from another program or computer, via a web browser, “Push” enables services to be *targeted* at the user, without them having to initiate the information collection activity. Instead, information finds the user. In other words, an automated retrieval of data from the Internet, corporate data sources

to or from a server site will (if unauthorised) involve the infringing act of reproduction, so liability will automatically arise at all actual or potential points where the protected material is made available.

⁴⁸⁰ For the distinction between push technology and pull technology, see Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 46 et seqq; Dan Jerker B Svantesson, 'The Characteristics making internet communication challenge traditional models of regulation – What every international jurist should know about the internet' (2005) 13 IJLIT 39-69.

and e-commerce web sites, is delivered directly to specific user populations in a personalised manner.⁴⁸¹ [*emphasis added*]

‘Pull’ technologies transmit data in response to an initiating and contemporaneous request from the user. On the internet, pull technologies are used when a user accesses a website; another example is network computing. In practice, many internet activities combine both forms of technology: email is transmitted to server by ‘push’ but the recipient’s email programme uses ‘pull’ to call for messages from the server.

Later in this chapter, I shall highlight aspects of push/pull technology in the context of the various torts committed. In my analysis of the torts, I shall try to separate out the various stages of the torts generally, and also, where appropriate, comment on whether they involve push or pull. In this regard, I have prepared a table (see Appendix 2) which sets out the three relevant torts and their various stages. For each of the stages of a tort, the table contains commentary on whether an infringement has actually been committed.

I feel it would be worthwhile, even at this early stage of the chapter, to give some brief examples of ‘push’ and ‘pull’ in the context of two of the rulings examined more closely later in the chapter.

Disseminating a number of defamatory emails is almost certainly push (given the generally accepted view that emails are push technology), but if the defamatory material is merely uploaded to a server (servicing a website) or to a blog, then that content needs to be pulled by a publishee before publication (and the related defamation) can occur. This ties in with the general view that *Dow Jones*⁴⁸² is authority for the proposition that digital content hosted on a web server is only deemed published at the point of access,

⁴⁸¹ Ecommerce Technology, ‘Push-Pull Technology’
<<http://ecommercetechnology.org/english/data/70.htm>> accessed 3 June 2014.

⁴⁸² *Dow Jones v Gutnick* [2002] HCA 56.

not at the point of storage.⁴⁸³ In other words, the publication and the attendant defamation only occur after a pull (by the publishee).⁴⁸⁴

Turning to the pivotal *Football Dataco v Sportradar*,⁴⁸⁵ and looking at the key notion of ‘reutilisation’ and its definition under Article 7 Database Directive, it has all the appearances of push. The definition refers to ‘any form of making available to the public all or a substantial part of the contents of a database by the distribution of copies, by renting, by online or other forms of transmission...’. However, later in the judgment, in particular at paragraph 21, the court refers to a person sending ‘by means of his web server, to another person’s computer, at that person’s request, data previously extracted from the content of a database protected by the *sui generis* right’. Despite the ruling referring to *a person* sending the data, it is not always entirely clear from the judgment if the data is sent by automated means or through the intervention of some individual. At this point, the process takes on more the appearance of pull. Furthermore, the resonance with copyright’s exclusive rights then becomes clear when the court states ‘by such a sending, that data is made available to a member of the public’.⁴⁸⁶

6.3 Copyright’s exclusive rights

Copyright is divided into a number of exclusive (or ‘restricted’) rights under both the UK and EU regimes. Under the UK copyright regime, and, more particularly, s 16 CDPA, 1988, copyright breaks down into six exclusive rights, namely:

1. The right to copy the work (defined in terms of reproduction in s 17);
2. The right to issue copies of the work to the public;
3. The right to rent or lend the work to the public;
4. The right to perform, show or play the work in public;

⁴⁸³ Andrew Murray, *Information Technology Law, The Law and Society* (2nd edn, OUP 2013) 175.

⁴⁸⁴ *Dow Jones v Gutnick* [2002] HCA 56 [44], where it is stated in the principal judgment that ‘...material on the World Wide Web is not available in comprehensible form until downloaded onto the computer of a person who has used a web browser to *pull* the material from the webserver’ (emphasis added).

⁴⁸⁵ Case C-173/11 *Football Dataco Ltd v Sportradar GmbH* [2013] CMLR 29. See para 3.6.4.

⁴⁸⁶ *Ibid* para 21.

5. The right to communicate the work to the public (defined in s 20 as including broadcasting and making available to the public by electronic transmission, etc.); and,
6. The right to make an adaptation of the work or to do any of the foregoing in relation to an adaptation.

It is interesting to note that the EU's topology for the exclusive rights, set out in Articles 2-4 inclusive of the InfoSoc Directive is quite different from the UK's. Article 2 refers to the reproduction right (equivalent to the right to copy a work under the UK regime). The communication to the public right and the making available right are bundled together in Article 3 with the making available constituent represented as a sub-component of the communication to the public right; this is the same as section 20, CDPA 1988, but no specific mention is made of performance in public. The WIPO Copyright Treaty, which the InfoSoc Directive implements,⁴⁸⁷ refers to communication and making available in the context of Arts 11, 11bis and 11ter Berne Convention (respectively, public performance/communication to the public, broadcasting, recitation). Lastly, Article 4 of the InfoSoc Directive refers to the distribution right.

6.4 The scope of my analysis in this chapter

My analysis will be restricted to the three exclusive rights that feature most prominently in UK/EU jurisprudence with a decided online character, namely, the reproduction right, the communication to the public right and the making available right.⁴⁸⁸ It should be noted from the outset that under both the WIPO Copyright Treaty and the Information Society Directive, the right of making available to the public is categorised as one

⁴⁸⁷ See InfoSoc Directive, recital (15).

⁴⁸⁸ Sterling argues that the two exclusive rights most affected by the internet are the reproduction right and the right of communication to the public. JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 653.

component of the more general right of communication to the public.⁴⁸⁹ This fact was reiterated very recently by the CJEU in the *Svensson* ruling.⁴⁹⁰

The making available right and its localisation in an online environment feature prominently in the 2013 European Commission Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society.⁴⁹¹ Later in this chapter, I critically evaluate the study's analysis of the making available right and the criteria it puts forward to localise this particular right in an online environment.

For reasons appearing in footnote format alongside each of the rights, my analysis will not cover the following UK exclusive rights:

- The right to issue copies of the work to the public⁴⁹²
- The right to rent or lend the work to the public⁴⁹³
- The right to perform, show or play the work in public⁴⁹⁴

⁴⁸⁹ Association Littéraire et Artistique Internationale, 'Report and Opinion on the making available and communication to the public in the internet environment: focus on linking techniques on the internet' *European Intellectual Property Review* (2014) 36 EIPR 149, 150. The specific provisions which provide for this situation are: Article 8 of the WIPO Copyright Treaty and Article 3(1) of the Information Society Directive.

⁴⁹⁰ Case C-466/12 *Svensson v Retriever Sverige AB* (ECJ (Fourth Chamber) 13 February 2014), paras 19 et seq.

⁴⁹¹ Severine Dusollier et al, 'Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society' (*European Commission*, 2013)

<http://ec.europa.eu/internal_market/copyright/docs/studies/131216_study_en.pdf> accessed 5 May 2014.

⁴⁹² This right applies only to tangible copies, see also Agreed Statement concerning Articles 6 and 7 WCT.

⁴⁹³ This right applies only to tangible copies.

⁴⁹⁴ As the term 'performance' is defined by Section 19(2)(b) of the CDPA as including 'any mode of visual or acoustic presentation, including presentations by means of a sound recording, film or broadcast of a work' it would appear, at first sight, that this exclusive right falls within the scope of my thesis. However, as demonstrated by the treatment of this

- The right to make an adaptation of the work or to do any of the foregoing in relation to an adaptation⁴⁹⁵

6.5 Conceptual Models

Both Svantesson and Sterling have propounded conceptual models which set out the various stages in an online defamation case and an online copyright infringement case, respectively. Svantesson's model is adequate to represent the situation in the UK,⁴⁹⁶ as

restricted right by Lionel Bently and Brad Sherman, *'Intellectual Property Law'* (3rd edn, OUP 2009) 146 et seqq, most of the related case law is from the 1880s through 1940s. In their analysis, Bently and Sherman do not cite any court ruling from the digital age. The sorts of scenarios that have been litigated under this right include the playing of a radio in the defendant's lounge (which could also be heard in a neighbouring restaurant) (*PRS v Camelo* [1936] 3 All ER 557); the operation of a jukebox (where the music played was not authorised); the performance of a play by an amateur dramatic club at Guy's Hospital (*Duck v Bates* [1884] 13 QBD 843), and, the performance of a musical work at the Embassy Club, London (*Harms (Incorporated) Ltd v Martans Club Ltd* [1927] 1 Ch 526). Given the clear pre-internet character of these rulings, it does not make sense to treat this exclusive right.

⁴⁹⁵ Under Section 21(3)(b) of the CDPA 1988, the term 'adaptation' (in relation to a musical work) is defined very narrowly to mean 'an arrangement or transcription of the work'. The terms 'arrangement' or 'transcription' have similar meanings and both imply an adaptation of a composition often involving the rewriting of a piece of music possibly for an instrument other than the instrument for which it was originally intended. Frequently, an arrangement involves significant changes to aspects of the original piece. A ruling that neatly encapsulates the key elements of an adaptation (in the context of a musical work) is *Francis Day & Hunter v Bron* [1963] 1 Ch 587. The principal elements mentioned therein were: the conscious or unconscious taking of a number of bars from the original work for use in a separate (allegedly infringing) work; considerable similarity between the two musical works; a requirement of proof of *de facto* similarity with the work alleged to be copied, and the principal musical influences of the alleged infringer. As the adaptation right, as defined by the CDPA 1988, has no obvious or natural connection with the BitTorrent file-distribution system, it seems appropriate not to analyse it in this chapter. While the author concedes that physically the files are 'delivered' in small portions (and said files emanate from a number of different downloaders), they will be 'collected' and reconstituted to create the original work, not an adapted version of the original work.

⁴⁹⁶ Svantesson's model is set out at pages 333 et seqq of his work, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012). As the model appears in the chapter titled 'Acritique of current rules of private international law' and has not been 'attributed' to any

is Sterling's, but the latter's model is restricted to the reproduction right. I shall use their models but critique same as I go along.

6.6 A definition of defamation and how it evolves through the case-law

Before examining Svantesson's conceptual model, I feel it would be beneficial to examine the tort of defamation and how it has evolved over the years,

Defamation involves a sequence of events with the actual primary or reputational harm really only occurring when the publishee reads (and comprehends) the defamatory material, and then only if it renders the publishee likely to hold the subject in 'hatred, ridicule or contempt', to cite the classic definition given in *Parmiter v Coupland*.⁴⁹⁷ The 2010 ruling of *Thornton v Telegraph Media Group Ltd* contains a good analysis of how the meaning of the term 'defamatory' has evolved over the decades.⁴⁹⁸ In *Thornton*, Tugendhat J defined 'defamatory' in the context of a statement as 'something which substantially affects in an adverse manner the attitude of other people towards the victim, or has a tendency to do so.'⁴⁹⁹

Tugendhat J also observed that the word 'attitude' in this definition 'makes clear that it is the actions of right-thinking persons that must be likely to be affected (so that they treat the claimant unfavourably, or less favourably than they would otherwise have done) not just their thoughts or opinions.'⁵⁰⁰ Although the definition of what is defamatory has evolved considerably over the last hundred years or so, by virtue of the case-law, it has always been premised on the perception of the publishee.⁵⁰¹

of seven States treated in Svantesson's work, one can assume that the model is neutral in character and does not 'belong' to any one of the seven countries. That said, there is absolutely nothing to suggest that the model is inappropriate to or unsuitable for the UK.

⁴⁹⁷ *Parmiter v Coupland* [1840] 6 M & W 105, 108, per by Lord Wensleydale (then Park B).

⁴⁹⁸ *Thornton v Telegraph Media Group Ltd* [2010] EWHC 1414 (QB) [28].

⁴⁹⁹ *Ibid* [95]. McBride and Bagshaw argue that the definition of 'defamatory' laid down by Tugendhat J in *Thornton v Telegraph Media Group*, is likely to be accepted as providing the core definition of what is defamatory. Nicholas J McBride and Roderick Bagshaw, *Tort Law* (4th edn, Pearson 2013) 530.

⁵⁰⁰ *Thornton v Telegraph Media Group Ltd* [2010] EWHC 1414 (QB) [91].

⁵⁰¹ Selected rulings which demonstrate the evolution include: *Tournier v National Provincial Union Bank of England Ltd* [1924] 1 KB 461, 477 (Scrutton LJ said that he did not think that Lord Wensleydale's classic definition was sufficient in all cases, because words could

6.7 Online Defamation

The steps in an online defamation case, as set out in Svantesson's conceptual model, follow hereunder.⁵⁰² Many of these steps are, in fact, an extension of Svantesson's model. My 'additions' can be seen by setting out the differences between Svantesson's model and the model which I have created. For instance, Svantesson starts his analysis with the offline world, I give primacy to the online world. His model does not refer to any case law while I enlist *Dow Jones v Gutnick*,⁵⁰³ the Lord McAlpine ruling⁵⁰⁴ and *Bier v Mines de Potasse*⁵⁰⁵ to highlight certain aspects or types of online defamation and, to give an example of a tort (albeit offline) which spreads beyond the borders of one country (e.g. *Bier*). For steps five and six, I provide a deeper level of analysis and provide a much larger number of examples of manifestation of harm to reputation and, consequential effects of defamation. Lastly, for each step, I confirm whether or not a defamation has actually been committed.

My analysis of each step comprises three elements:

- a. The online situation

damage the reputation of a man as a business man which no one would connect with hatred, ridicule or contempt); *Youssouf v Metro-Goldwyn Mayer Pictures Ltd* [1934] 50 TLR 581, 587 (Slessor LJ expanded the *Parmiter v Coupland* definition to include words which cause a person to be shunned or avoided); *Sim v Stretch* [1936] 2 All ER 1237, 1240 (Lord Atkin expressed the view that the definition in *Parmiter v Coupland* was probably too narrow. He proposed a new test: would the words tend to lower the plaintiff in the estimation of right-thinking members of society generally?); and *Drummond-Jackson v British Medical Association* [1970] 1 All ER 1094, 1104 (Lord Pearson stated that in some cases, it is necessary to consider the occupation of the plaintiff as 'words may be defamatory of a trader/business man or professional man if they impute lack of qualification, knowledge, skill, capacity, judgment or efficiency in the conduct of his trade or business or professional activity...' (even if they do not impute any moral fault or defect of personal character)).

⁵⁰² Dan Jerker S Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 333 et seqq.

⁵⁰³ *Dow Jones v Gutnick* [2002] HCA 56.

⁵⁰⁴ *Lord McAlpine of West Green v Sally Bercow* [2013] EWHC 981 (QB).

⁵⁰⁵ Case 21/76 *Handelskwekerij G J Bier BV v Mines de Potasse d'Alsace SA* [1976] ECR 1735. See para 4.2.3.2.

- b. The offline situation (the offline equivalent of ‘a’)
- c. A statement on whether a defamation has occurred.

Step One

Online:

The defamatory material is composed. The composer drafts a defamatory email or drafts a defamatory piece and saves same on an electronic file with the intention of publishing it on a blog or online bulletin board the following day.

Offline:

The defamatory material is written in a letter or is published in a magazine. In the former case, the letter is placed in an envelope but is not yet posted. In the latter case, the magazines are stored in the warehouse of the publisher, awaiting delivery to newsagents.

Has defamation occurred?

As the defamatory material has not yet been sent to potential publishees, there has been no publication and therefore no defamation.

Step Two - The defamatory material is disseminated or dispatched

Online:

The author clicks on ‘send’ on his email (or, tweets the defamatory statement,⁵⁰⁶ or, posts same to facebook or writes same on a blog). In each case, the defamatory material is posted to a server somewhere.

Offline equivalent:

The letter containing the defamatory material is posted to a third party or the magazines containing the defamatory material are loaded onto vans for delivery to newsagents.

Has defamation occurred?

At this point, the defamatory material is being transmitted but has not yet been received or comprehended by the publishee. Therefore, no defamation has yet occurred.

⁵⁰⁶ See generally, *Lord McAlpine of West Green v Sally Bercow* [2013] EWHC 981 (QB).

Step 2 A

Online:

The defamatory material is stored on a server. This step is not included in Svantesson's model, but I have included it due to it being an intrinsic part of the technological process and the fact that there is an important parallel in the context of online copyright infringement. The server may be located locally or abroad. Just because the material is uploaded in country A does not necessarily mean that it will be stored on a server in country A. Later in this chapter, in my analysis of the making available right, it will become evident that there can be a disconnect between location of upload and location of storage of the uploaded material.

Offline:

The defamatory material is stored in the newsagents' warehouse or, in the case of the defamatory letter, is stored in the Royal Mail's sorting office.

Has defamation occurred?

At this point, the defamatory material has not yet been comprehended by the publishee. Hence, no defamation has occurred.

Step Three

Online:

The publishee takes possession of the defamatory material. For instance, the recipient receives the e-mail in his inbox, or accesses the relevant website, but has not yet read/comprehended the email or the content of the website.

Offline equivalent:

The publishee buys the newspaper or retrieves his post containing the defamatory statement(s), but decides to read it later.

Has a defamation occurred?

No defamation has occurred as the publishee has not yet read or comprehended the defamatory material.

Step Four

Online:

The publishee reads and comprehends the defamatory material (the material enters his mind). He reads the e-mail or, he accesses the blog/discussion board and reads the defamatory material.

Offline equivalent:

The purchaser of the newspaper reads the relevant article or the letter is read by its recipient.

Has a defamation been committed?

At this stage, a defamation has usually been committed as the defamatory material has been comprehended by the publishee.⁵⁰⁷

Step Five

The harm to reputation starts to manifest itself.⁵⁰⁸ In effect, the publishees and those with whom they communicate start to hold the subject in hatred, ridicule or contempt. The nature and degree of the harm can vary. It is surmised that the harm could range from the ridiculing or criticising of the victim in an intemperate or exaggerated fashion, to the victim's views not being taken seriously by his peers (with consequences for his credibility, both privately and professionally

⁵⁰⁷ The principal judgment in *Dow Jones v Gutnick* is very clear on this point. It states 'harm to reputation is done when a defamatory publication is comprehended by the reader, the listener, or the observer. Until then, no harm is done by it'. *Dow Jones v Gutnick* [2002] HCA 56 [26]. Later in the principal judgment (at [44]), the court states that defamation is to be located at the place where the damage to reputation occurs. Ordinarily, that will be where the allegedly defamatory material is available in comprehensible form assuming, of course, that the person defamed has in that place a reputation, which is thereby damaged.

Then, referring explicitly to 'material on the World Wide Web' (also at [44]), the court states that such material is not available in comprehensible form until downloaded onto the computer of a person who has used a web browser to pull the material from the webserver. It is where that person downloads the material that the damage to reputation may be done.

⁵⁰⁸ Under UK defamation law, libel is actionable in itself without adducing additional evidence. Injury to the plaintiff's reputation is sufficient.

Step Six

The plaintiff feels the effects of the consequences.

Unlike the previous steps, step six is less specific and may comprise a number of different acts. Step six occurs when the effects of the consequences of the defamation are felt by the victim. For example, the defamed victim may lose his job. He may lose business opportunities. His business may suffer without actually becoming insolvent (sales, profitability, or turnover may decrease). His marriage or personal relationships may suffer and, his credibility among the wider business community/society in general may be affected. In addition, the victim of the defamation may suffer emotional injury, depression or even suicidal ideation.

If the victim has business ventures in a number of different States and all are negatively affected by the defamatory comments, then the harmful effects are felt in multiple jurisdictions. In a way, the harmful effects are ‘localised’ in each country where the victim has business interests. From a tort perspective, defamation can only occur in a jurisdiction if the claimant (victim) has an established reputation there. As regards the issue of multi-state torts, the ECJ ruling in *Handelskwekerij G J Bier v Mines de Potasse d’Alsace SA*⁵⁰⁹ is particularly relevant as the defendant’s negligent actions in France resulted in harmful effects downriver in the Netherlands. It is also one of the key conflicts rulings in that it gives claimants a greater choice in terms of where to sue, under Article 5(3), Brussels I.

6.8 Online Copyright Infringement

In this section, I will deal with the second element in the critical evaluation - online copyright infringement. I shall focus initially on the principal exclusive right, the reproduction right, and later treat the communication to the public right, and the making available right. Fortunately, as regards the reproduction right, I can draw on Sterling’s conceptual model,⁵¹⁰ though arguably it is not quite as comprehensive as Svantesson’s defamation model. That said, it does indicate the *loci* of unauthorised reproductions.

⁵⁰⁹ Case 21/76 *Handelskwekerij G J Bier BV v Mines de Potasse d’Alsace SA* [1976] ECR 1735, and treated in depth at para 4.2.3.2.

⁵¹⁰ JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 659 et seq.

My research will demonstrate the different criteria used by the courts to localise infringements of the 3 selected exclusive rights. More importantly, it will highlight points of disconnection as between online defamation and online copyright infringement and, indeed, between the exclusive rights *inter se* when it comes to localising the respective torts. It will become apparent that different rules and criteria are used to localise infringements of the three different exclusive rights.

Sterling's conceptual model provides a succinct and clear analysis of the *loci* of infringements of the reproduction right in an internet context. The model refers to illegal reproduction occurring at five different stages of the *unauthorised* transmission or incorporation of copyright material.⁵¹¹ I have introduced a sixth stage, referring to the effects of the consequences of copyright infringement. This is to maintain the symmetry with the online defamation component.

Step One

Reproduction occurs where protected material is incorporated into the uploader's computer (in the hard drive or RAM or both).

This is most likely to be an infringement of the rightholder's reproduction right as it involves the initial copying without authorisation. However, if the reproduction were to fall under one of the permitted acts under sections 28A to 31 of the CDPA 1988 or under one of the copyright exceptions due to come into force in the UK on 1st June 2014, then it would be legal notwithstanding lack of authorisation. A good example of a form of reproduction that would be saved by the new set of exceptions is the creation of personal copies for private use.⁵¹²

⁵¹¹ JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 659.

⁵¹² The changes to the copyright exceptions in the UK are introduced by way of secondary legislation in the form of five statutory instruments that amend relevant sections of the CDPA 1988. The five S.I.s are: The Copyright and Rights in Performances (Personal Copies for Private Use) Regulations 2014; The Copyright and Rights in Performances (Quotation and Parody) Regulations 2014; The Copyright and Rights in Performances (Disability) Regulations 2014; The Copyright and Rights in Performances (Research, Education, Libraries and Archives) Regulations 2014; and The Copyright (Public Administration) Regulations 2014.

Step Two

Reproduction takes place in the transmission process between the infringer's computer and the server site. This occurs when a copy of the infringing material passes through a number of intermediary servers⁵¹³ on its way to the server site.

This thesis argues that the inherent unlawfulness of the initial reproduction persists the whole way through the transmission process right up to the point at which the infringing copy reaches the server site or, final destination. Stated differently, once the initial reproduction is an unauthorised one, all subsequent incidental reproductions along the digital chain of distribution (i.e. copies created on the intermediary servers) take on an illegal character too and are not saved by the exceptions provided for in Article 5(1) of the InfoSoc Directive.⁵¹⁴

Viewing the above situation from the perspective of an ISP, it is submitted that an ISP would, most likely, be in a position to avail of the 'mere conduit' and 'hosting' safe harbour exemptions provided by Articles 12 and 14 respectively of Directive 2000/31/EC (the E-Commerce Directive) provided of course it satisfies the conditions therein.

Article 12 specifically refers to the 'automatic, intermediate and transient storage of the information transmitted'. The provision goes on to specify that the storage takes place for the 'sole purpose of carrying out the transmission in the communication network' and that the information is 'not stored for any period longer than is reasonably necessary for the transmission'. It is submitted that this is the type of storage that occurs on an intermediary server and, for that reason, the ISP will not be liable for the information transmitted.

⁵¹³ Sterling refers to these points as the intermediary transmission points. See JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 666.

⁵¹⁴ Article 5(1) of the InfoSoc Directive creates an exemption to the reproduction right in respect of temporary acts of reproduction which are transient or incidental in nature, form an integral part of a technological process, whose sole purpose is to enable a transmission in a network between third parties by an intermediary, and which have no independent economic significance.

In terms of the exemptions for hosting provided by Article 14, it is argued that an ISP operating intermediary servers which store (host) unauthorised transient reproductions could avail of the hosting exemption. The key condition is that the ISP does not have actual knowledge of the illegality of the material hosted and that it is not aware of facts or circumstances from which the illegal activity or information is apparent (Article 14(1)(a)). As it is very unlikely that an ISP would have actual knowledge of transient illicit reproductions on its intermediary servers, it would, almost certainly, satisfy the conditions for an exemption under Article 14. At this juncture, it is important to distinguish between actual knowledge (of illegal activity) and presumed awareness on the part of the ISP.

Most ISPs are presumably aware of the fact that transient reproductions occur on their intermediary servers as a matter of course. These reproductions are part and parcel of the technological process and, in this regard, similar to the copies that are created on a laptop's RAM when its owner accesses websites. Clearly, ISPs are aware of this fact *but* can this general awareness of technological realities be equated with actual knowledge of illegalities? It is contended that such an equating would be both unreasonable and unfair.

A general awareness of the existence of infringing copies on one's intermediary servers is still a far way off 'actual knowledge of illegal activity'.⁵¹⁵ To develop the point, if an ISP were required (by law, for instance)⁵¹⁶ to instantly identify infringing copies on one or more of its intermediary servers, it would, most likely, experience significant difficulties in doing so. For one, it can really only know what constitutes an infringing copy if it also knows what the (original) copyright material is. But there is an additional step. It must also know that the original material was copied without the licence of the rightsholder. To expect this level of knowledge and awareness on the part of the ISP is unrealistic and the ISP's position is assisted by the following three elements:

- Article 15(1) E-Commerce Directive (no general obligation to monitor);

⁵¹⁵ E-Commerce Directive, art 14(1)(a).

⁵¹⁶ Article 15(2) of the E-Commerce Directive permits Member States to establish obligations for information society service providers promptly to inform the competent public authorities of alleged illegal activities undertaken by recipients of their service.

- the CJEU's rulings in *Scarlet v Sabam*⁵¹⁷ and *Sabam v Netlog*⁵¹⁸ in which it held that an ISP and the owner of an online social network respectively could not be obliged to install a general filtering system in order to prevent its subscribers from unlawfully using protected works; and
- the Opinion of Advocate-General Cruz Villalón in the recent ruling, *UPC Telekabel v Constantin Film* in which he stated: 'It would constitute such an inadmissible measure if the court had ordered the ISP actively to seek copies of the infringing page among other domain names or to filter all the data carried in its network in order to ascertain whether they constitute transfers of specific protected film works and to block such transfers'.⁵¹⁹

Step Three

Reproduction taking place at the server site.

Once again, viewed from the perspective of an ISP, this form of reproduction is most likely to fall under the scope of the hosting immunity contained in Article 14, E-Commerce Directive. This form of reproduction is also likely to result in a more permanent form of storage and it is interesting to note that both Article 12 (mere conduit) and Article 13 (caching) of the E-Commerce Directive refer to 'intermediate and transient storage' and 'intermediate and temporary storage' respectively, but this type of temporary/transient storage is not referred to at all in Article 14.

So long as the ISP which is providing the hosting service under Article 14 of the E-Commerce Directive ('storage of information provided by a recipient of the service', in the words of Article 14) does not have actual knowledge of illegal activity or information and is not aware of facts or circumstances from which the illegal activity or information is apparent, then it will not be liable for the information stored at the request of a recipient of the service. The immunity under Article 14 will be lost if the

⁵¹⁷ Case C-70/10 *Scarlet v Sabam* [2011] ECR I-11959.

⁵¹⁸ Case C-360/10 *Sabam v Netlog* [2012] 2 CMLR 18.

⁵¹⁹ Case C-314/12 *UPC Telekabel Wien v Constantin Film*, Opinion of AG Cruz Villalón (26 November 2013) para 78.

ISP, upon obtaining knowledge or awareness of infringing material on its server, fails to act expeditiously to remove or disable access to the infringing material.⁵²⁰

Step Four

Reproduction taking place in the transmission process between the server site and the point of access.

In reality, this could be classified as a *retransmission* as the infringing material originated at a point other than the server.⁵²¹ It is argued that such temporary reproduction could avail of the exception under Article 5(1) of the InfoSoc Directive. This provision holds that temporary acts of reproduction which are transient or incidental, an integral part of a technological process, and which have no independent economic significance are exempted from the reproduction right provided for in Article 2 of the InfoSoc Directive.⁵²²

Step Five

Reproduction which takes place in the accessor's computer (in the RAM or hard disk) or on the receiving PC's/laptop's/smart device's screen.

⁵²⁰ It should be noted that from June to September 2012, the European Commission engaged in a public consultation titled 'A Clean and Open Internet' on procedures for notifying and acting on illegal content hosted by online intermediaries.

⁵²¹ Sterling argues that the issue of whether a transmission originates at the server site or is retransmitted from that locus will influence questions of liability for unauthorised use, either at the originating point, or, in the case of retransmissions, at the initiating point or at the retransmission point or at both points. See, JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 150.

⁵²² Hector L MacQueen, 'Appropriate for the Digital Age? Copyright and the Internet: 1 Scope of Copyright' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009) 192. There are some interesting parallels between the temporary reproductions which occur along the transmission process between server and point of access, and the act of browsing the internet. As regards temporary copies produced while browsing the internet, the UK Supreme Court held in *Public Relations Consultants Association Limited v the Newspaper Licensing Agency Limited* [2013] UKSC 18 [33] that such temporary copies (whether for private or commercial use) do not infringe copyright.

Step Five is further nuanced by the issue of local rightholder's authorisation. If the local rightholder has not granted authorisation for use in each of the receiving countries, then infringement of the reproduction right may be held to occur at every point of unauthorised access to, or recording of material by means of access to a server site.⁵²³

Step Six

While the consequential effects of online copyright infringement are not explicitly described in Sterling's conceptual model, they do arise. The effects may negatively impact the rightholder's financial wellbeing or, his reputation. This is the consequential harm, which needs not be proven to establish liability for copyright infringement but rather goes to quantum. Unauthorised copies, disseminated free of charge online, may erode actual or potential royalties payable to the copyright owner. Where the piracy is significant, possibly of a commercial scale, and this becomes public knowledge, this fact may undermine licensing opportunities for the rightholder. Where the rightholder is a large body corporate, widescale piracy may damage company reputation and goodwill, with knock-on effects for external financing such as equity stakes and seed capital. If the rightholder is a listed company, the share price may fall. Furthermore, it is possible that sufficiently proximate 'downstream' damage will found jurisdiction in the State where it occurs, under Article 5(3), Brussels I.

6.9 Points of connection/disconnection between online defamation and online infringement of the reproduction right

6.9.1 Points of Connection:

From the viewpoint of an ISP and the exemptions available to it under the E-Commerce Directive, there is a perfect crossover between online defamation and online copyright infringement. The Article 12 ('mere conduit') and Article 14 ('hosting') exemptions are available in cases of both defamatory material and copyright infringing material provided the relevant conditions under those provisions are satisfied by the ISP. As regards the mere conduit exemption, this would extend to the 'automatic, intermediate and transient storage' of the infringing material (whether defamatory or, copyright infringing) on the communication network (Article 12(2), E-Commerce Directive).

⁵²³ JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 660.

6.9.2 *Points of Disconnection:*

One significant disconnect between online infringement of the reproduction right and online defamation is the ‘delayed’ harmful event in the latter. In effect, in defamation cases, injury only occurs after the publishee has comprehended the defamatory material. In an online context, a considerable amount of time may elapse before the recipient (publishee) opens the defamatory email. For example, he may be on holiday and therefore not accessing his email or there may be a technical fault with his laptop, thereby preventing him from accessing his email. But, the crucial point is that the cause of action does not accrue to the victim until the harm has been committed (i.e. the publishee has comprehended the defamatory material). This potentially delayed cause of action contrasts with an online copyright infringement where the cause of action arises the instant the protected material is infringed. In other words, the online copyright infringement becomes actionable at an earlier stage (potentially, much earlier stage) than the online defamation.

In addition, in copyright infringement cases, there is no requirement that there be third party involvement (i.e. the publishee). Infringement of copyright material occurs once the act of primary infringement occurs – there is no requirement that a recipient takes possession of the infringing material. The commission of the tort in an online IPR scenario is more immediate than in an online defamation scenario.

One could argue that the immediate actionability of the online copyright infringement is more theoretical than real, *but*, with the growing number of torrent tracking sites, this increases the likelihood of infringing copies being discovered soon after their creation. Interestingly, a 2012 study conducted by Birmingham University indicates that an illegal file-sharer downloading popular content would be logged by a monitoring firm within three hours.⁵²⁴

In the UK, another disconnect exists by virtue of the single publication rule contained in section 8 of the Defamation Act 2013. This rule replaces the old multiple publication rule and ensures that republications of the original defamatory statement (or,

⁵²⁴ BBC, ‘BitTorrent study finds most file-sharers are monitored’ (*BBC New Technology*, 4 September 2012) <<http://www.bbc.co.uk/news/technology-19474829>> accessed 24 May 2014.

substantially the same statement) fall within the initial time limit (for the purpose of the Limitation Act 1980) as the original defamatory statement. This contrasts with peer-to-peer infringements where one infringing content file can constitute the basis of a number of distinct actionable claims. In general in the UK, a copyright owner will have a right of action under section 17 (the reproduction right) and section 20 (communication to the public) of the CDPA 1988.⁵²⁵

6.10 Communication to the Public

I now turn to the second exclusive right that I shall deal with, the communication to the public, and the relationship of the general concept with its subcomponent, the making available right.

The issue of localising unauthorised online communications to the public has been considered at length by Arnold J in the web-blocking judgments critically evaluated at in chapter 7 (from para 7.3.5 onwards). To date, there have been five such judgments.

Not all of these rulings deal with the issue of localisation and some analyse the issue in more depth than others. In effect, there are three rulings which are of particular relevance to the issue of localisation. They are, in chronological order:

Dramatico Entertainment Limited v British Sky Broadcasting,⁵²⁶
EMI Records Limited v British Sky Broadcasting Limited,⁵²⁷ and
Football Association Premier League Limited v British Sky Broadcasting.⁵²⁸

It would be fair to say that whilst *Dramatico* ventilated the issue of localisation of the communication to the public right, it did so without engaging in a particularly deep analysis. To use the well-worn colloquialism, it got the ball rolling in terms of considering the localisation of this exclusive right in an online environment, and highlighted the lack of clarity in the Court of Justice's jurisprudence.

⁵²⁵ See *Dramatico Entertainment Ltd v British Sky Broadcasting Ltd* [2012] EWHC 268 (Ch) [40]–[43] (the reproduction right) and [44]–[71] (communication to the public right).

⁵²⁶ *Dramatico Entertainment Limited v British Sky Broadcasting* [2012] EWHC 268 (Ch).

⁵²⁷ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch).

⁵²⁸ *Football Association Premier League Limited v British Sky Broadcasting* [2013] EWHC 2058 (Ch).

In contrast, both *EMI Records* and *Football Association Premier League*, genuflecting as they do to *Football Dataco*,⁵²⁹ engage in a comprehensive analysis of the matter of localisation, placing particular emphasis on the notion of targeting the public in the UK and the various factors that indicate that targeting has taken place. I shall now analyse each of the three relevant rulings.

6.10.1 *Dramatico Entertainment Limited v British Sky Broadcasting*

The first of the rulings to examine the issue of localisation in the context of the communication to the public right is *Dramatico Entertainment Limited v British Sky Broadcasting*.⁵³⁰

In that case, Arnold J, referred to the UK Court of Appeal's reference to the CJEU in *Football Dataco v Sportradar*.⁵³¹ Despite that case relating to the Database Directive (Directive 96/9/EC), it was, in Arnold J's mind, relevant, as the national reference was essentially asking whether an extraction and/or re-utilisation of data from a database occurs in the location from where the data is transmitted (the emission theory⁵³²) or in the location where it is received (the transmission theory).

While he acknowledged that those questions did not concern Article 3(1) of the Information Society Directive (which provides for the communication to the public right), he did draw an important parallel between the two principal questions referred to the CJEU in *Football Dataco* and the confusing and inconsistent jurisprudence of the CJEU in relation to Article 3(1) of the Information Society Directive.⁵³³ Mr Justice Arnold summed up the parallel by referring to the claimants' contention that under Court of Justice case-law, it was unclear whether a communication to the public under Article 3(1) occurs where the communication originates or where it is received (or perhaps both).⁵³⁴ This consideration was important in *Dramatico Entertainment Limited*

⁵²⁹ Case C-173/11 *Football Dataco Ltd v Sportradar GmbH* [2013] CMLR 29.

⁵³⁰ *Dramatico Entertainment Limited v British Sky Broadcasting* [2012] EWHC 268 (Ch).

⁵³¹ See para 3.6.4.

⁵³² Or 'push' in the terminology outlined previously.

⁵³³ *Dramatico Entertainment Limited v British Sky Broadcasting* [2012] EWHC 268 (Ch) [67].

⁵³⁴ *Ibid* [67].

in the context of the claim against the operators of The Pirate Bay website (under Section 20, CDPA 1988) as The Pirate Bay's servers were located outside the UK.⁵³⁵

However, ultimately, Arnold J accepted the claimants' submission that the stark choice between place of origination and place of reception was immaterial as the evidence made clear that the UK users were involved as both uploaders and downloaders.⁵³⁶ But, that begs the question, would Arnold J have felt compelled to make a choice between place of origination (Step 2 in the scheme used above) and place of reception (step 4) if say, there had been no uploaders in the UK or, alternatively, no downloaders in the UK? *Dramatico* also emphasised a distinction between Art 3(1) of the Infosoc directive, which provides authors with redress against communication to the public, and Art 3(2) which provides the owners of copyright in entrepreneurial works (related rights) with redress only against making available.⁵³⁷ In subsequent paragraphs, it was stated that the right of communication should be construed broadly. Where the cases do not clearly distinguish between the two, it is suggested that the court's findings are probably directed to the making available right. In *Dramatico* itself, the first claimant represented holders of rights in sound recordings.

6.10.2 *EMI Records Limited v British Sky Broadcasting Limited*⁵³⁸

Again, the claimants in this case were relying on rights in sound recordings. The High Court examined the issue of communication to the public from two perspectives: that of the users of the websites and, that of the operators of the websites.

As regards the users of the websites, described as 'uploaders' by Arnold J, the judge had no difficulty finding that they communicate the claimants' sound recordings to the public since they make the recordings available by electronic transmission in such a way that members of the public could access the recordings from a place and at a time individually chosen by them,⁵³⁹ in this case actively mediated by the peer-to-peer software. In terms of determining whether the act of communication to the public occurred in the UK, the claimants contended that localisation in the UK occurred in two

⁵³⁵ Ibid.

⁵³⁶ Ibid [68].

⁵³⁷ Ibid [67].

⁵³⁸ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch).

⁵³⁹ Ibid [39].

situations: (i) where the person making the work available (the uploader) is located in the UK (step 2); and (ii) where the recipient of the work (the downloader) is located in the UK (step 4).⁵⁴⁰

In a passage of his ruling which is somewhat unclear,⁵⁴¹ Arnold J, influenced by the court ruling and the Advocate-General's Opinion in *Football Dataco Ltd v Sportradar GmbH*,⁵⁴² states that localisation in the UK of the act of communication to the public occurs where the uploader is located in the UK (i.e. Step 2).⁵⁴³ He then expresses doubt that there is an act of communication in the UK where the recipient of the work is located in the UK (step 4), as he was unconvinced that the acts of communication by the uploaders were targeted at members of the public in the UK.⁵⁴⁴ This requirement of targeting members of the public (a notion that featured prominently in an IP context in *Football Dataco*)⁵⁴⁵ is amplified at a later stage in the judgment when Mr Justice Arnold applied it separately to website operators. It is submitted that this 'targeted push' analysis actually takes into account both step 2 and step 4; this becomes apparent when one looks at the criteria used to assess 'targeting'. It is consistent with the definition of the making available right, which refers to demand from users.

In his examination of the issue of communication to the public from the perspective of website operators,⁵⁴⁶ Mr Justice Arnold addressed the matter of whether the acts of communication to the public had occurred in the UK⁵⁴⁷ and whether they had been targeted at a public in the UK.

⁵⁴⁰ Ibid [41].

⁵⁴¹ Ibid [33]-[41].

⁵⁴² Case C-173/11 *Football Dataco Ltd v Sportradar GmbH* [2013] CMLR 29; Case C-173/11 *Football Dataco v Sportradar GmbH*, Opinion of AG Cruz Villalón (21 June 2012).

⁵⁴³ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch) [41].

⁵⁴⁴ Ibid.

⁵⁴⁵ Case C-173/11 *Football Dataco Ltd v Sportradar GmbH* [2013] CMLR 29, paras 39–47.

⁵⁴⁶ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch) [44]–[51].

⁵⁴⁷ Para 63 of the judgment is particularly revealing as to the truly international character of the three P2P file-sharing websites' activities. For example, in the three years prior to this ruling and in a bid to frustrate international investigations and evade copyright enforcement actions, KAT repeatedly shifted between different service providers in eight different countries, namely France, Germany, Luxembourg, Poland, Romania, Spain, Sweden and Ukraine. This

Referring to *Football Dataco v Sportradar*, Arnold J believed that it was relevant to take into account, by analogy, criteria which the CJEU had considered as relevant to the issue of targeting the public in a number of other mainly non-copyright contexts. In that regard, he listed the following relevant rulings: *Joined Cases Pammer v Reederei Karl Schlüter, and Hotel Alpenhof v Heller*;⁵⁴⁸ *L'Oreal SA v eBay International*⁵⁴⁹ and, *Donner*.⁵⁵⁰

Mr Justice Arnold then proceeded to refer to a key passage in *Pammer and Hotel Alpenhof*⁵⁵¹ in which the ECJ set out a non-exhaustive list of matters capable of constituting evidence that a trader's activity is being directed to the Member State of the consumer's domicile.⁵⁵²

form of jurisdiction hopping was also embraced by both H33T and Fenopy, with the latter showing a particular penchant for the US, Japan and Canada.

⁵⁴⁸ *Joined Cases C-585/08 and C-144/09 Pammer v Reederei Karl Schlüter, and Hotel Alpenhof v Heller* [2010] ECR I-12527 (Article 15 of Brussels I - when is a trader's activity on a website directed to the Member State where the consumer is domiciled?).

⁵⁴⁹ *Case C-324/09 L'Oreal SA v eBay International* [2011] ECR I-6011 (Article 5 of Council Directive 89/104/EEC (the Trade Marks Directive), and Article 9 of Council Regulation 207/2009/EC (The Community Trade Mark Regulation) – An offer for sale of goods (involving an unauthorised use of a trade mark) targeted at consumers located in the territory covered by the trademark. Targeting was evident in this case by way of the offer for sale being accompanied by details of the geographic areas to which the seller was willing to dispatch the product (para 65 of the judgment).

⁵⁵⁰ *Case C-5/11 Criminal proceedings against Titus Alexander Jochen Donner* [2012] OJ C250/05, para 29 (Article 4 of the Information Society Directive - A trader directing his advertising (both online and offline) at members of the public. The goods advertised were illegal replicas of copyright-protected furnishings in the so-called Bauhaus style. The directing or targeting was denoted by the following factors: the existence of a German language website, the content and distribution channels of Dimensione's advertising materials and its cooperation with Inspem, as an undertaking making deliveries to Germany).

⁵⁵¹ *Joined cases C-585/08 and C-144/09 Pammer v Reederei Karl Schlüter, and Hotel Alpenhof v Heller* [2010] ECR I-12527, para 93.

⁵⁵² *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch) [50]. See para 2.10 of this thesis in relation to the non-exhaustive list of matters.

This thesis argues that the analogy of an e-trader directing his activities to a specific country is not particularly strong. This is linked to the fact that the matters accepted by the court in *Pammer and Hotel Alpenhof* as constituting evidence of trader activity being directed to the Member State of the consumer's domicile are, quite understandably, peculiar to the world of e-commerce. But, this in a way begs the question: how useful would such evidential factors be in the distinct and significantly different world of digital copyright infringement?

Objectively speaking, some of the evidential factors deemed acceptable in *Pammer and Hotel Alpenhof* (listed at para 93 of that judgment) seem either too generic or irrelevant to be of much use in the specific context of online communications to the public. Examples of such evidential factors include:

- The international nature of the activity
- The mention of itineraries from other Member States for going to the place where the trader is established
- Mention of telephone numbers with an international code
- Use of a top-level domain name other than that of the Member State in which the trader is established
- Mention of an international clientele composed of customers domiciled in various Member States.

Admittedly, the factors of foreign language and currency were deemed to constitute good evidence of directing activities to/targeting the public in both *Pammer/Hotel Alpenhof* and *EMI Records* but that is meagre commonality in the overall scheme of things.

Another consideration weakens the analogy of the e-trader/e-commerce. The notion of activity 'directed to' (in Article 15(1)(c) Brussels I) is not defined in that regulation. Nor was it defined in the predecessor Brussels Convention. It must therefore be interpreted independently, by reference principally to the system and objectives of the

regulation.⁵⁵³ The absence of a clear definition dilutes the parallels and makes the analogy both weaker and less dependable.

Returning to the specific issue of localisation of the communication to the public, Arnold J accepted the claimants' contention that the communications to the public occurred in the UK by virtue of their being reasonably clearly targeted at the public in the UK.⁵⁵⁴ The factors that influenced the court as to targeting were as follows:

1. There was a large number of users of each website in the UK;
2. A substantial portion of the visitors to each website were from the UK;
3. The recordings listed on each of the websites include large numbers of both (a) recordings by UK artists and (b) recordings that are in demand in the UK;
4. The default language of each of the websites was English;
5. In addition, in the case of KAT, it included advertisements with prices in sterling.⁵⁵⁵

6.10.3 Football Association Premier League Limited v British Sky Broadcasting⁵⁵⁶

In this case, the offending website, FirstRow, operated as an indexing and aggregation portal to streamed broadcasts of sporting events. Mr Justice Arnold had to determine whether the communication to the public actually took place in the UK as FirstRow's website was hosted in Portland in Sweden,⁵⁵⁷ a well-known haven for pirate sites.

Referring back to his ruling in *EMI Records Limited v British Sky Broadcasting* Arnold J reiterated that if the communication originates from outside the UK, then it must target the public in the UK for it to be localised in the UK.⁵⁵⁸ The claimant, FAPL, relied on the following matters as evidencing an intention on the part of the operators of FirstRow to target the public in the UK:

⁵⁵³ Case C-96/00 *Rudolf Gabriel* [2002] ECR I 6367 para 37.

⁵⁵⁴ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch) [51].

⁵⁵⁵ *Ibid.*

⁵⁵⁶ *Football Association Premier League Limited v British Sky Broadcasting* [2013] EWHC 2058 (Ch).

⁵⁵⁷ *Ibid* [21].

⁵⁵⁸ *Ibid* [31].

- I. The website is an English language website.
- II. The advertising on FirstRow includes adverts for companies located in the UK and products consumed in the UK.
- III. FirstRow provides access to a large number of competitions which are extremely popular with UK audiences. In particular, the amount of Premier League content on the website is up to 11% whilst a Premier League match is being played.
- IV. FirstRow is a very popular website in the UK.
- V. Between 12 and 13.7% of the worldwide traffic to FirstRow's website comes from the UK.
- VI. FirstRow is discussed on internet blogs and forums, where a significant proportion of the internet traffic to those blogs and forums comes from the UK.⁵⁵⁹

Arnold J had no difficulty accepting the foregoing elements as evidencing an intention by FirstRow to target the public in the UK. Ultimately, Arnold J held that there was both an unauthorised communication to the public by FirstRow in the UK and an infringement by it of FAPL's copyrights.⁵⁶⁰

6.11 Points of connection/disconnection

One significant point of disconnection between the localisation of online communication to the public and online defamation is the requirement that there be a targeting of the public in the former. In the Section 97A cases analysed earlier, it was this targeting of a UK public that localised the tort in the UK, thereby justifying assumption of jurisdiction by the UK courts.

In applying the 'targeting the public' test, the English High Court uses predominantly commercial and social/cultural factors, for example, language; advertising, popularity of the website, origin of internet traffic to the infringing website and, blogs/forums which discuss the infringing website. Once these verifiable factors are proven, then it is almost certain that localisation will 'follow' these factors. This appears to be a hybrid analysis when compared with defamation and reproduction, but it is consistent with the principle

⁵⁵⁹ Ibid [45].

⁵⁶⁰ Ibid [46] et seq.

that infringements are best stemmed as close to source as possible. It tends to point to a single location, or at least fewer locations than a download criterion. Online defamation, on the other hand, may be quite a bit more difficult to prove and localise.

In effect, with defamation, the tort only occurs when a defamatory publication is comprehended by the reader, listener or the observer.⁵⁶¹ In terms of online defamation, there is the requirement that the defamatory material be available in ‘comprehensible form’ and this really only occurs when the material is downloaded onto the computer of the publishee (the publishee will pull the material from the webserver).⁵⁶² In short, the place of download is where the damage to reputation will occur. As a corollary, the place of download is equivalent to *locus delicti*.

But, the commission of an online defamation invariably occurs in a private setting, where the publishee downloads the defamatory material on his PC, laptop, i-Phone etc. Given that the commission of the tort is dependent on a private and discrete act by the publishee (i.e. accessing/downloading the defamatory material), then arguably it is less easy to localise compared with a communication to the public, where, the relevant factors are more public and therefore more easily ascertainable.

For example, in *EMI Records*, factors deemed relevant to deciding whether there was an intention to target the public included (among others): the language of the website; the nature of the advertising on the offending website and, the popularity of the website. All of these factors are easily verifiable. The website’s popularity can, for instance, be checked using the online measurement company, Nielsen. All in all, therefore, the process of localisation for communication to the public is a simpler and more straightforward process.

It is somewhat ironic too that it is not a copyright case that provides inspiration for the targeting of the public requirement, rather a database right case – *Dataco v Sportradar*. Further, Mr Justice Arnold looked beyond *Football Dataco v Sportradar* and highlighted EU rulings relating to e-commerce, unauthorised use of a trade mark and,

⁵⁶¹ *Dow Jones & Company v Gutnick* [2002] HCA 56 [26].

⁵⁶² *Ibid* [44].

online/offline advertising of goods which infringed copyright, all of which dealt with criteria on targeting of the public.

6.12 Right of making available to the public: the views of various commentators

As stated earlier,⁵⁶³ the right of making available to the public is categorised as one component of the more general right of communication to the public. As there is no formal guidance on localisation of this right in the relevant legal instruments, it is left to law practitioners and academics to postulate theories about the localisation of the online act of making available.

6.13 Possible application of the communication theory and the emission theory

Sterling submits that the communication theory (formulated originally in the context of broadcasting) should be applied to determine localisation in the context of making available.⁵⁶⁴ In short, this theory holds that the making available to the public takes place, *inter alia*, at the point of reception, or Step 4 in the scheme of my earlier analysis. This approach is also consistent with any factual, logical or linguistic interpretation of the circumstances. In reality, where digital copyright material is transmitted over the internet and received by members of the public such material is made available to the public where reception takes place. As the making available right is an on-demand right, the making available occurs when the public accesses the material from a place and at a time individually chosen by them, as per the wording of Article 3(1) of the Information Society Directive. In effect, this means that when infringing material is placed on a website, it will be made available at every point where there is a computer, smartphone, tablet etc which can access the infringing material.

The alternative to the communication theory is the emission theory. However, its application in an online environment would be neither practical nor practicable. Unlike a satellite broadcast transmission system which involves an identifiable transmission point, the internet involves multiple transmission points.⁵⁶⁵ Locating the point of initial transmission for an internet communication may be exceedingly difficult to achieve. To exacerbate matters, the relevant material may have been stored on multiple servers (mirror servers) and/or physically located in a country other than the country where the

⁵⁶³ At para 6.3

⁵⁶⁴ JAL Sterling, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008) 469.

⁵⁶⁵ *Ibid.*

relevant service provider is located. In some ways, the ruling in *Dow Jones & Company v Gutnick* is apposite. There, the appellant loaded its material for its online journal onto six different servers. As it happened, all six servers were located in the same jurisdiction i.e. the state of New Jersey, but the situation could have been very different. It is not unknown for websites to be run off servers located in different countries.

6.14 Where the making available right takes place according to Sterling

Sterling argues that making available on the internet takes place at the following three places:

1. At the place where the content provider transmits material to a server site, or provides material for online transmission to an end user
2. At the server site
3. At the reception point or points at which an item of subject matter which is available online is or may be accessed.⁵⁶⁶

While the places described at ‘2’ and ‘3’ can, with justification, be considered places of making available, the author finds it difficult to understand how the places mentioned in ‘1’ can be used to, in effect, localise an online act of making available.

In terms of ‘1’ above, it has to be borne in mind that the act of making available occurs once the public has the possibility to access the content.⁵⁶⁷ It is difficult to see how the mere transmission of content to a server site or the mere provision of material to *an* end user actually constitute making available. The former example is but a provision of the material to the website. That material still has to be uploaded/loaded onto the website (by the operators of that website) before it can be accessed by the public and before an actual act of making available occurs. Once uploaded, the material becomes actually or potentially available to the public.

⁵⁶⁶ Ibid 471 et seq.

⁵⁶⁷ Séverine Dusollier et al, ‘Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society’ (*European Commission*, 2013) 33 <http://ec.europa.eu/internal_market/copyright/docs/studies/131216_study_en.pdf> accessed 5 May 2014. See also, Jorg Reinbothe and Silke von Lewinski, *The WIPO Treaties 1996* (Butterworths Lexis Nexis 2002) 108.

As regards the latter example, it refers to provision of material to just one end-user. This thesis argues that the provision of material to an individual is unlikely to be deemed a making available to the public. A number of ECJ rulings have indicated that the term ‘public’ means a fairly large number of people.

For example, in June 2005, in its ruling in *Mediakabel BV v Commissariaat voor de Media*⁵⁶⁸ in the context of television broadcasting, the ECJ described the ‘public’ as ‘an indeterminate number of potential television viewers to whom the same images are transmitted simultaneously’.⁵⁶⁹ One month later, in *Lagardère Active Broadcast v SPRE*,⁵⁷⁰ the ECJ in the context of satellite broadcasting used the same formula again (‘an indeterminate number of potential listeners’) to describe the public. However, it went further in that it stated that a ‘limited circle of persons’ cannot be regarded as part of the public.⁵⁷¹

Even more compelling is the CJEU’s ruling in *Società Consortile Fonografici v Marco Del Corso*⁵⁷² where the court was interpreting the concept of communication to the public in the context of the InfoSoc Directive. At paragraph 84 of its judgment, the CJEU refers to its earlier rulings in *Mediakabel*, *Lagardère Active Broadcast* and *SGAE*⁵⁷³ and sums them up as implying that the term ‘public’ means a ‘fairly large number of persons’.⁵⁷⁴ In attempting to define ‘public’, the court refers to the WIPO Glossary which interprets the concept of communication to the public as meaning ‘making a work...perceptible in any appropriate manner to persons in general, that is, not restricted to specific individuals belonging to a private group’.⁵⁷⁵

⁵⁶⁸ Case C-89/04 *Mediakabel BV v Commissariaat voor de Media* [2005] ECR I-4891.

⁵⁶⁹ *Ibid* para 30.

⁵⁷⁰ Case C-192/04 *Lagardère Active Broadcast v SPRE* [2005] ECR I-7199.

⁵⁷¹ *Ibid* para 31.

⁵⁷² Case C-135/10 *Società Consortile Fonografici v Marco Del Corso* (ECJ (Third Chamber) 15 March 2012).

⁵⁷³ Case C-306/05 *Sociedad General Autores y Editores de España (SGAE) v Rafael Hoteles SA* [2006] ECR I-11519.

⁵⁷⁴ Case C-135/10 *Società Consortile Fonografici v Marco Del Corso* (ECJ (Third Chamber) 15 March 2012), para 84.

⁵⁷⁵ *Ibid* para 85.

Returning to the criterion of ‘a fairly large number of people’, the CJEU states that this notion is intended to indicate that the concept of public encompasses ‘a certain *de minimis* threshold, which excludes from the concept groups of persons which are too small or insignificant’.⁵⁷⁶

Cumulatively, *MediaKabel*, *Lagardère* and *Società Consortile Fonografici* send out a clear signal about the meaning of the term ‘public’. Small, insignificant groups of persons do not constitute a ‘public’ and a *de minimis* threshold will apply. Clearly, therefore, an individual will not constitute a ‘public’.

6.15 European Commission’s Localisation Criteria for the Making Available Right

A 2013 European Commission-funded study on the application of the InfoSoc Directive proposes comprehensive localisation criteria for the making available right. The study proposes three different localisation criteria for the making available right. They are:

1. Where the servers are located on which the works are hosted
2. Where the uploader has his centre of interests; and
3. Where the material act of upload has taken place.⁵⁷⁷

I shall now examine and critically evaluate the three criteria in the light of *Sterling’s* older proposed places of localisation.

6.16 Criterion No. 1 - Location of the servers upon which the works are hosted (step 3)

The European Commission’s views this criterion negatively. It points out that it may be difficult to determine in which country the servers are located.⁵⁷⁸ In addition, the works

⁵⁷⁶ Ibid para 86.

⁵⁷⁷ Séverine Dusollier et al, ‘Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society’ (*European Commission*, 2013) <http://ec.europa.eu/internal_market/copyright/docs/studies/131216_study_en.pdf> accessed 5 May 2014.

⁵⁷⁸ Ibid 135. This point was also made in Case C-173/11 *Football Dataco Ltd v Sportradar* [2013] CMLR 29, para 45.

may be ‘spread’ over different servers in different countries, meaning that one act of making available would be situated in several countries (in effect, no single location).⁵⁷⁹ Practically speaking, even the uploader may not be aware of the country in which the servers are located. Also, an infringer could exploit this criterion by using servers located in a Member State whose laws offer weak protection to rightholders in terms of judicial remedies.⁵⁸⁰

6.17 Criterion No. 2 – Centre of activities of the uploader: establishment, domicile or habitual residence (no correspondence with the ‘step’ analysis)

This criterion proposes that the act of making available be localised at the uploader’s ‘centre of activities’. The European Commission Study posits that a legal person has its centre of activities ‘at its establishment’ (this would most likely equate with the English law notion of the seat of the company) while a natural person has his centre of activities at his domicile or habitual residence.⁵⁸¹

Applying this criterion, it matters not where the uploader was actually physically situated when the material act of making available was effected.⁵⁸² The legal act of making available will be localised in the Member State where the individual has his

⁵⁷⁹ Séverine Dusollier et al, ‘Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society’ (*European Commission*, 2013) 135 <http://ec.europa.eu/internal_market/copyright/docs/studies/131216_study_en.pdf> accessed 5 May 2014.

⁵⁸⁰ Ibid.

⁵⁸¹ Ibid. Interestingly, the SatCab Directive also applies an establishment criterion in cases where there is ‘no use of an uplink station situated in a Member State’, but a broadcasting organisation established in a Member State has commissioned the act of communication to the public by satellite. Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15, art 1(2)(d)(ii).

⁵⁸² Séverine Dusollier et al, ‘Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society’ (*European Commission*, 2013) 135 <http://ec.europa.eu/internal_market/copyright/docs/studies/131216_study_en.pdf> accessed 5 May 2014.

domicile/habitual residence or, where the company has its place of establishment.⁵⁸³

The types of scenario envisaged are the following:

- A music service provider with a complex, international structure, established in Member State A (localisation criterion) but whose acts of upload are performed in Member State B
- An individual is domiciled in Member State A (localisation criterion) but he uploads material in Member State B (while holidaying there or whilst on a business trip there).⁵⁸⁴

In both instances, the localisation criterion (centre of activities) will have no link with the material acts that defined the act of making available.

6.17.1 The Advantage of using this criterion

The advantage of this approach is that the act of making available is localised in just one Member State even if it has effects in a number of Member States (the effects may include commercialisation or accessibility of the work abroad). In addition, the place of upload is disregarded in favour of place of domicile/habitual residence, or establishment. As the uploader's centre of activities is generally relatively easy to determine, this criterion increases legal certainty.⁵⁸⁵

The benefits of this legal certainty become apparent in certain situations. For example, take the example of the commercial exploitation of a particular work (to which the making available right relates) across the territories of several Member States without the targeting of a public in a specific country. Another example is where several national exploitations are arranged in respect of the same work. In both cases, use of the protected work occurs in more than one EU Member State but, by virtue of this criterion, its making available right is localised in the Member State which constitutes the uploader's centre of activities.

⁵⁸³ Ibid.

⁵⁸⁴ Ibid 136.

⁵⁸⁵ Ibid 135.

6.17.2 Some problems arising from use of this criterion

The use of this criterion is not without its problems. If Member State A is the uploader's centre of activities but Member State B is the place of actual upload, then the latter will be deprived of any regulatory power or influence over the act of upload even though the upload occurred on its territory. Moreover, there may be no significant link between the country of establishment and the country where the work is actually made accessible to the public by virtue of it being uploaded.

To many, it may seem counterintuitive that the country of exploitation (upload) is relegated in terms of importance and 'displaced' by the country of establishment. Furthermore, this criterion delinks localisation from effects (of the making available right). For some, this disconnect between localisation and effects (of one of copyright's exclusive rights) may seem illogical and inconsistent, particularly in the light of the key tort jurisdictional rule contained in Brussels I.

This rule, contained in Article 5(3), Brussels I, refers to cases of tort or delict and gives the plaintiff the right to sue the tortfeasor 'in the courts for the place where the harmful event occurred or may occur'. This thesis argues that under Article 5(3), jurisdiction is linked to the harmful event but that there is only a thin demarcation between the harmful event and the effects that flow from same. In short, the tort (the harmful event) and its effects are strongly intertwined.

It follows that Article 5(3) indirectly attaches considerable importance to the effects of the commission of a tort. In the light of this PIL rule, the criterion of the uploader's centre of activities, which de-emphasises effects and which opts instead for the uploader's establishment/domicile/habitual residence seems to be somewhat of an outlier. To conclude, another risk associated with applying the centre of activities-criterion is that a copyright infringer could purposely choose to establish its centre of activities in a Member State with relatively weak copyright protection in terms of judicial remedies, etc. The net effect of such establishment-shopping is that any infringement of a making available right would be localised in that particular Member State (of establishment) and would therefore be subject to the weaker copyright law prevailing there.

6.18 Criterion No 3 – Where the material act of upload is initiated (Step 2)

According to this criterion, the act of making available takes place where the material act of upload of the works is initiated. This is the place where the user/uploader is actually based when he transmits the protected work to the server, knowing that it will lead to the work being available to the public.⁵⁸⁶ To use a practical example, the upload process for YouTube entails accessing the video file upload page, signing into one's YouTube account, clicking the yellow 'Upload' button, locating the relevant video file (which one wishes to upload) on one's PC, etc. and then opening same. Once the spinning circle appears, one knows that the upload process has begun. In this example, the act of making available takes place in the country where the uploader is physically located when he engages in the above described process.

It goes without saying that the act of upload may occur at a location other than the place of establishment of a company or the domicile/habitual residence of a natural person. For example, a company may have a place of establishment in Member State A, but 3 further operational branches in Member States B, C, and D. For operational reasons, the company may decide to upload protected material in Member State D. In such a case, the making available is effected from a country other than the uploader's place of establishment. Important too is the fact that the place of upload is not always coterminous with the place where the server is located as a work can be uploaded in Member State A, but stored on a server in Member State B.⁵⁸⁷

Arguably this criterion represents an attempt to return to the unitary-right model first assayed by the Cable and Satellite Directive, whereby the location of a broadcast for copyright/licensing purposes was identified as the single State of uplink. As Hugenholtz observed, encryption and licensing practices prevented the hoped-for single market in broadcasting from developing from this.⁵⁸⁸ Hugenholtz also predicted that the Cable and Satellite Directive would be overtaken by digitisation. Thus, rights would follow the InfoSoc Directive, which, in his view 'reflects a traditional territorial approach'. However, his observation on encryption has been addressed by the CJEU in *FAPL v*

⁵⁸⁶ Ibid 137.

⁵⁸⁷ Ibid.

⁵⁸⁸ Bernt Hugenholtz, 'Copyright without Frontiers: is there a future for the Satellite and Cable Directive' (*IViR*, 2005)
<<http://www.ivir.nl/publications/hugenholtz/copyrightwithoutfrontiers.pdf>> accessed 13 June 2014

*QC Leisure*⁵⁸⁹ and related caselaw. Furthermore, as my research has shown (at 6.10 to 6.10.3), by adopting a ‘targeted push’ model of online communication to the public, the web-blocking cases have avoided the most fragmented version of the purely territorial approach that would flow from following *Dow Jones v Gutnick*.⁵⁹⁰ These cases have put online communication to the public on a jurisdictional footing similar to cable and satellite, in a way which is compatible with the ‘new public’ approach of *FAPL v QC Leisure* (analysed at para 3.6.1.).

6.18.1 Some problems associated with this criterion

Like criterion number 2, this criterion is not problem-free when it comes to its application. For example, it may be difficult to pinpoint the country where the act of upload took place. For a commercially significant service provider running, for example a trans-European music service or online video service, acts of upload may be performed at different locations in different Member States.⁵⁹¹ As a consequence, its operations will be governed by several laws which the service provider needs to factor into its commercial operations. A similar problem may transpire in the case of user platforms whereby the platform provider concludes an agreement with rightholders for content uploaded by individual users.⁵⁹² Once again, the likelihood exists that the content could be uploaded in different Member States so it would be difficult to indicate one location for the upload. Lastly, this criterion is susceptible to location shopping whereby uploaders (especially commercial service providers) may structure their organisation taking into account the weakest copyright protection.⁵⁹³

6.19 Points of connection/disconnection between Sterling and the European Commission Study on the making available right

6.19.1 Points of connection

Both Sterling and the European Commission suggest that the making available right could be localised at the place where the server (upon which the works are hosted) is located, though the European Commission views this criterion rather negatively due to the possible difficulties in actually determining the location of the servers. Separately,

⁵⁸⁹ At para 3.6.1.

⁵⁹⁰ This ruling is analysed from para. 9.3.1. on

⁵⁹¹ *Ibid* 138.

⁵⁹² *Ibid*.

⁵⁹³ *Ibid* 139.

the European Commission also foresees problems from a localisation perspective where the relevant material is ‘spread’ over different servers in different countries.

6.19.2 Points of disconnection

Sterling draws some inspiration from the broadcasting sector and considers both the communication theory and the emission theory in the context of localising the making available right. In endorsing the communication theory, he, in essence, implicitly accepts that the making available takes place at the point of reception. In rejecting the emission theory, Sterling essentially rejects the theory’s lack of practicality in an online setting. The absence of an identifiable transmission point and the real risk of the infringing material being stored on multiple servers are both problematical for localisation, in Sterling’s eyes. In contrast, the European Commission’s study makes no reference to either the communication theory or the emission theory.

The only criterion for localisation that focuses on a person rather than a location is the European Commission’s criterion of: Where the uploader has his centre of interests. In elaborating on this criterion, it is unfortunate that the Commission seems to regard the notions of ‘domicile’ and ‘habitual residence’ as being one and the same. To a certain extent, this is understandable as Brussels I (at Article 60) uses the connecting factor of domicile while Rome I (at Recital (39) and Article 19) and Rome II (at Article 23) use the connecting factor of habitual residence. In a way, the Commission’s study has created an ‘amalgam’, but, most likely, an imprecise one! This is explicable by the differences in definition of the terms ‘domicile’ and ‘habitual residence’ in the EU’s PIL framework. For example, the term ‘domicile’ (for the purposes of a company), as defined in Article 60, Brussels I, is broader than the definition for ‘habitual residence’ under Rome I and Rome II. Under Brussels I, a company’s domicile can mean its statutory seat, or, its central administration or, its principal place of business. In contrast, under Rome I and Rome II, the habitual residence of a company is defined more narrowly as ‘place of central administration’.

6.20 Conclusions

6.20.1 Reproduction right versus Defamation

As regards online infringement of the reproduction right and online defamation, there are more points of disconnection than points of connection. In short, it would seem that online defamation does not read so easily onto online infringement of the reproduction

right. The principal point of connection between the two torts exists at the level of the ISP. Under the E-Commerce Directive, the ISP could avail of exemptions under Articles 12 (mere conduit) and 14 (hosting) for both defamatory material and content which infringes the reproduction right in copyright.

One significant disconnect between infringement of the reproduction right and defamation is the ‘delayed’ harmful event in the latter. Defamation cases require the publishee to comprehend the defamatory material before the injury arises. This (necessary) third party involvement can slow down the commission of the tort and have a negative knock on effect for the cause of action. This potentially delayed cause of action contrasts with an online copyright infringement where the cause of action arises the instant the protected material is infringed. In sum, the infringement of the reproduction right potentially becomes actionable at a much earlier stage than defamation. Analysed from a different angle, online copyright infringement cases do not require the ‘intervention’ of a third party (i.e. publishee, in the case of defamation) for the cause of action to accrue.

Nor should the benefit of immediate actionability of online copyright infringement be dismissed lightly. The recent growth in the number of torrent tracking sites increases the likelihood of a rightholder discovering quite quickly that his copyright material has been infringed, particularly if he uses the services of a monitoring firm.

6.20.2 Online Communication to the public versus online defamation

One significant point of disconnection between the localisation of online communication to the public and online defamation is the requirement that there be a targeting of the public in the former. In the Section 97A cases analysed in chapter 7, it was this targeting of a UK public that localised the tort in the UK, thereby justifying assumption of jurisdiction by the UK courts.

When applying the ‘targeting the public’ test, the English High Court uses predominantly commercial and social/cultural factors, for example, language; advertising and origin of the internet traffic. As these factors are readily verifiable, a decision on localisation can be taken speedily.

In contrast, when it comes to online defamation, the commission of the tort often occurs in a private setting. The tort takes place when the publishee downloads (and comprehends) the defamatory material. But, this will often involve a discrete and private act by the publishee, something considerably less verifiable than the factors outlined for targeting the public above. In essence, this means that localising an act of online defamation is more difficult to achieve than localising an online communication to the public, primarily because the factors to be verified in the latter are more public and therefore more ascertainable.

6.20.3 The Making Available Right

Sterling versus European Commission Study

There is commonality between Sterling and the European Commission in terms of possibly localising the making available right at the place where the server (upon which the works are hosted) is located. However, the European Commission also expresses some scepticism about this criterion as it acknowledges possible difficulties in determining the actual location of the servers. These difficulties could be exacerbated if the infringing material is spread over different servers in different countries. While Sterling considers the two classic broadcasting theories – the communications theory and the emission theory – in the context of localising the making available right, he ultimately rejects the emission theory as he does not believe it to be practicable in an online setting. Factors that make the emission theory unworkable according to Sterling are: the absence of an identifiable transmission point and the risk of the infringing material being stored on multiple servers. In endorsing the communications theory, Sterling implicitly accepts that the making available takes place at the point of reception. In contrast with Sterling, the European Commission makes no reference to either of the broadcasting theories in its study.

Chapter 7. Jurisdictional Issues: Article 2, Brussels I

Facilitative Elements

7.1	Introduction.....	208
7.2	Article 2, Brussels I.....	209
7.3	The Facilitative Elements.....	213
7.3.1	The First Facilitative Element - Norwich Pharmacal Relief	213
7.3.2	Case law featuring Norwich Pharmacal relief.....	214
7.3.2.1	Coca Cola Company v British Telecommunications plc	214
7.3.2.2	Totalise plc v Motley Fool Ltd.....	215
7.3.2.3	Takenaka (UK) v Frankl Ltd.....	215
7.3.2.4	Mitsui & Co Ltd v Nexen Petroleum UK Ltd.....	216
7.3.2.5	Grant v Google UK Ltd.....	216
7.3.2.6	Smith v ADVFN plc	217
7.3.2.7	Media C.A.T. v Adams and Others.....	217
7.3.2.8	Rugby Football Union v Viagogo Ltd	219
7.3.2.9	Golden Eye (International) Ltd v Telefonica UK Ltd.....	220
7.3.3	Digital Economy Act 2010.....	223
7.3.4	Technical Measures Legislation in France and the Republic of Ireland .	224
7.3.4.1	France.....	224
7.3.4.2	The Republic of Ireland	224
7.3.5	Section 97A CDPA 1988 and Blocking of Websites	225
7.3.5.1	Twentieth Century Fox v British Telecommunications (Newzbin 2)	226
7.3.5.2	Twentieth Century Fox v British Telecommunications (No 2)	226
7.3.5.3	Dramatico Entertainment Limited v British Sky Broadcasting Limited (2 rulings; February and May 2012).....	227

7.3.5.4 EMI Records Limited v British Sky Broadcasting Limited (2013)	229
7.3.5.5 The Football Association Premier League v British Sky Broadcasting Limited	231
7.3.5.6 Paramount Home Entertainment v British Sky Broadcasting.....	234
7.3.5.7 Overblocking.....	237
7.3.6 The Second Facilitative Element – Geolocation Technology	237
7.3.7 The Various Uses of Geolocation.....	238
7.3.8 Geolocation as an enforcement tool	238
7.3.9 Ensuring compliance with territorially-limited copyright laws.....	239
7.3.10 Limiting access to online content from abroad	241
7.3.11 The Accuracy of Geolocation Technology.....	241
7.3.12 Accuracy of Geolocation Technologies Impugned	245
7.3.13 The Growing Influence of Geolocation Technology in the Courts.....	247
7.3.14 Possible Legal Obstacles to the use of Geolocation Technology.....	251
7.3.15 Some Conclusions on Geolocation Technology.....	255
7.4 The Third Facilitative Element – Data Retention Legislation.....	257
7.4.1 How Directive 2006/24/EC was implemented into UK law	258
7.4.2 Data Retention (EC Directive) Regulations 2009	259
7.4.3 The communications data to be retained under the Schedule to the Regulations.....	259
7.4.4 CJEU’s ruling in Digital Rights Ireland	261
7.4.5 A Preliminary Ruling concerning the validity of Directive 2006/24/EC	261
7.4.6 The General absence of limits	263
7.4.7 The data retention period.....	263
7.4.8 Interference with the fundamental rights set out in the Charter	263
7.4.9 The rules relating to security and protection	264
7.4.10 Outcome of the case	265
7.4.11 Implications of the ruling	265
7.4.12 The Anti-Terrorism, Crime and Security Act 2001.....	267
7.5 Conclusions.....	268

Chapter 7. Jurisdictional Issues: Article 2, Brussels I Facilitative Elements

*'On the Internet, nobody knows that you're a dog.'*⁵⁹⁴

*Regularly, when the law is challenged by new technical developments, the question arises whether the same technology causing the problem can also provide the means for their solution.*⁵⁹⁵

7.1 Introduction

In this chapter and the subsequent two chapters, I shall focus on the practical difficulties of applying the tort jurisdictional rules (contained in Brussels I) to the internet. In essence, this intermeshing analysis, spanning all three chapters, will cover two provisions of the Brussels I Regulation, namely, Article 2 and Article 5(3). As defendant identification is a key element of Article 2, I have divided the analysis into both facilitative elements and non-facilitative elements. To ensure the demarcation, I have devoted a separate chapter to each of the two elements. Consequently, facilitative elements are treated in this chapter and non-facilitative in the next. The term 'facilitative' refers to factors which facilitate the application/operation of Article 2 while 'non-facilitative' means the converse.

This chapter will argue that, in reality, Article 2, Brussels I is reliant on a number of 'props' for its efficacy - technology (geolocation technology), *Norwich Pharmacal* relief, and data retention legislation (inspired by the EU but transposed into domestic law). As regards the last-mentioned element, considerable confusion now reigns after the recent CJEU ruling which held Directive 2006/24 to be invalid.

⁵⁹⁴ Citation from a cartoon by Peter Steiner, 'On the Internet, nobody knows you're a dog' (1993) 69 *The New Yorker* 61 (emphasis added). It is used by Myriam van Dellen, 'Anonymity on the Internet. What does the Concept of Anonymity Mean?' (2002) 9 *EDI LR* 1 to indicate that in principle we are anonymous on the Internet.

⁵⁹⁵ Dorothee Thum and Torsten Bettinger, 'Territorial Trademark Rights in the Global Village – International Jurisdiction, Choice of Law and Substantive Law for Trademark disputes on the Internet: Part 1' (2000) 31 *IIC* 162, 164 (emphasis added).

The ‘undercurrent’ of technology runs through this chapter and the next. These two chapters demonstrate that technology can potentially be used by both the IP owner (as claimant) and the infringer to assist their aims/actions. For example, geolocation technology may assist the claimant while the dynamic allocation of IP addresses (discussed in chapter 8) may assist the infringer in that it can make the obtaining and production of strong digital evidence more challenging. In effect, chapters 7, 8, and 9 of this thesis constitute a synthesis of the relevant technologies, laws and common law relief that can be used by the copyright holder to bring a civil case against infringers and by the infringer to potentially evade detection/prosecution.

The provisions in Brussels I that will be examined in this series of three inter-related chapters are:

1. Article 2, Brussels I (facilitative elements) [this chapter];
2. Article 2, Brussels I (non-facilitative elements) [chapter 8]; and
3. Article 5(3), Brussels I [chapter 9].

Each of the aforementioned elements is contained in a discrete chapter. In terms of Article 2, Brussels I, I have decided to examine the facilitative elements before the non-facilitative elements primarily because the ‘evidence’ supporting the facilitative elements is stronger than the evidence supporting the non-facilitative elements. As Article 2 constitutes the basic jurisdictional rule in the Brussels I regime, it is both logical and practical to examine it before treating the special jurisdiction rule in Article 5(3), the latter being an exception to the fundamental principle of suing the defendant in the place of his domicile. As is the norm in most cases involving PIL, jurisdiction is decided before the applicable law and I shall honour that tradition in this thesis.

7.2 Article 2, Brussels I

I shall now proceed to analyse the basic rule in the EU jurisdictional framework, namely, Article 2, Brussels I. This rule provides that the defendant *shall* be sued in the courts of the Member State in which he is domiciled.⁵⁹⁶ This provision presupposes that the defendant has already been identified. But the identification of the infringer is

⁵⁹⁶ The actual wording of Article 2, Brussels I is ‘Subject to this Regulation, persons domiciled in a Member State shall, whatever their nationality, be sued in the courts of that Member State.’

considerably more complicated in the online world than in the offline world.⁵⁹⁷ Stated more forcefully, the process of establishing a person's offline identity from their online identity constitutes a significant evidentiary and legal hurdle.⁵⁹⁸ To give a practical example: a copyright infringer may use several computers or several infringers may use the same computer, thereby making identification of the culprit very difficult. Difficulties may also arise with local networks. There, several computers in a local network are connected to the internet through a gateway or firewall which performs *network address translation* (NAT). They all appear to have the IP address of the gateway or firewall, which is responsible for redistributing the traffic coming from the internet (using ports).

In an internet environment, personal computers, WAP-enabled mobile phones and PDAs with internet connectivity can all act as a smokescreen from the perspective of the online copyright infringer. Nor is it unknown for online infringers to access a modem in another country or State (in the case of the US) by way of a long-distance phone call.⁵⁹⁹ All these elements make user identification extremely challenging.

It may be possible for the injured copyright holder using geolocation technology⁶⁰⁰ and the IP address⁶⁰¹ of the infringer to trace the copyright infringement to a geographic

⁵⁹⁷ See for example, Mark D Evans, 'Protection of Data on the Internet' (2002) 1 IPQ 50, 74 where the author states:

The law is willing to provide recourse for those in situations where even sophisticated technological remedies have failed to protect website content. As has been shown, two of the most commercially important markets to British business, Europe and America, have developed various means to do so. To gain access to such recourse, one must first know whom to sue, and this is often not a trivial issue, given the worldwide accessibility of the Internet.

⁵⁹⁸ Ian Walden, 'Forensic Investigations in Cyberspace for Civil Proceedings' (2004) 18 Int'l Rev L Computers & Tech 275 et seq.

⁵⁹⁹ Dick Thornburgh and Herbert S Lin, 'A Global Internet' in Dick Thornburgh and Herbert S Lin (eds), *Youth, Pornography and the Internet* (National Academy Press 2002) 66; Henrik Spang-Hanssen, *Cyberspace & International Law on Jurisdiction: Possibilities of Dividing Cyberspace into Jurisdiction with Help of Filters and Firewall Software* (DJØF Publishing 2004) 338, fn 1190.

⁶⁰⁰ Geolocation services attempt to pinpoint Internet users' locations based on their network addresses. In other words, the technology enables the linking of Internet Protocol (IP)

location. On the basis of scholarly writings on geolocation technologies, it seems that this technology has become increasingly more sophisticated and perhaps now accurate down to street level.⁶⁰²

Of course, narrowing the possibilities to a certain street is one thing but that still leaves the injured copyright holder with the difficult task of determining the identity of the infringer who disseminated the infringing material online or via an internet-enabled mobile phone.⁶⁰³ Unfortunately, for the copyright holder, internet communications (and non-subscription-based mobile phones) allow a high degree of anonymity to be achieved.⁶⁰⁴

addresses to physical addresses (countries, cities and even postcodes). 'Geography and the net – Putting it in its place' *The Economist* (9 August 2001) 18-20.

⁶⁰¹ This procedure may also require the co-operation of a potentially large number of separate ISPs who would play a role in tracing the Internet routes of infringing data packets. However, the situation in the EU is quite confusing now following the recent CJEU ruling in [name of case]. Following the CJEU's finding that the Data Retention Directive was invalid, there is an element of uncertainty as to what implications this ruling will have for the individual data retention regimes in the EU and for ISPs in general; . The intricate nature of the tracing process is demonstrated by the fact that even viewing a small web page may require thousands of data packets to be transmitted and each packet would need to be tracked individually, as the paths taken by the individual packets are quasi-random and dependent on many factors. Mark D Evans, 'Protection of Data on the Internet' (2002) 1 IPQ 50, 60.

⁶⁰² Dan Jerker Svantesson, 'Geo-Location Technologies and other Means of Placing Borders on the "Borderless" Internet' (2004) 23 J Marshall J Computer & Info L 101, 137; Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 399 where that author argues that geolocation technologies are sufficiently accurate to be taken into account for legal purposes.

⁶⁰³ The Freedom Phone is a totally anonymous mobile phone. Its anonymity is safeguarded by the fact that it contains no spy chip (receiver) amenable to the GPS satellite navigation system. It is sold by the company PT Shamrock. PT Shamrock, 'PT Freedom Phone™- Anonymous Mobile & (GSM) Sim Card – The hassle of anonymous call sending and receiving SOLVED' <<http://www.ptshamrock.com/auto/freedomphone.htm>> accessed 5 July 2012.

⁶⁰⁴ Chris Nicoll, 'Concealing and Revealing Identity on the Internet' in C Nicoll, JEJ Prins and MJM van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions - Information Technology & Law Series 2* (1st edn, Asser Press 2003) 100, where the author states as follows: As a general rule, Internet communications exist at the end of the anonymity spectrum most favourable to concealing identity and face-to-face contact exists at the least favourable end.

A determined copyright infringer can achieve online anonymity with relative ease. In addition, tracing internet traffic requires the assistance of ISPs. Even if an ISP is able to trace certain internet communications (transmission of infringing material) to a specific computer, the copyright holder will still face problems if the computer in question is a public computer (located for instance in an internet café, transport hub (airport/train station), public or university library). Where the trace leads to a privately owned computer, the injured copyright holder is in a stronger position as hopefully the ISP's logs would be sufficient to inculcate the infringer.⁶⁰⁵ If not, a forensic analysis of the PC could be carried out but this could take six months before the results are known.

Before proceeding to examine the facilitative elements, it is helpful to firstly describe the three main components which make up the facilitative element. They are:

1. *Norwich Pharmacal* relief;
2. Geolocation Technology; and
3. Data Retention Legislation

'POT' or 'plain old telephone' is somewhere in between but closer to least favourable - a rough placing it shares with orthodox mail. On the other hand, cellular phones of the disposable variety can provide high levels of anonymity.

For a decidedly theoretical analysis of the concepts of anonymity and identity, see MJM van Dellen, 'Anonymity on the Internet. What does the Concept of Anonymity Mean?' (2002) 9 EDI LR 1-6. To obtain an insight into the concepts of anonymity and identity, the author distinguishes between the following five categories: a. non-perceptibility of the subject; b. legally non-relevant anonymity, c. legally relevant anonymity, d. legally non-relevant identity, and, e. legally relevant identity.

⁶⁰⁵ See *Polydor Limited v Brown* [2005] EWHC 3191 where it was held that a father who had no knowledge that his children had downloaded P2P software and copied music files containing copies of copyright works in a shared directory onto his computer, was liable for infringement under CDPA 1988, s 20 on the basis that he had breached the copyright holder's exclusive right to communicate the work to the public.

7.3 The Facilitative Elements

7.3.1 *The First Facilitative Element - Norwich Pharmacal Relief*

The first facilitative element lies in the English rules of civil procedure. The standard procedure for a claimant to obtain identification information is through the so-called *Norwich Pharmacal* jurisdiction.⁶⁰⁶ This judge-made relief was established by the House of Lords in *Norwich Pharmacal v Customs and Excise Commissioners*. In that case, Reid LJ stated the principle upon which the doctrine was based as follows:

If through no fault of his own a person gets mixed up in the tortious acts of others so as to facilitate their wrongdoing, he may incur no personal liability, but he comes under a duty to assist the person who has been wronged by giving him full information and disclosing the identity of the wrongdoers.⁶⁰⁷

Norwich Pharmacal orders will not be available where the information may be obtained by other means.⁶⁰⁸

This form of equitable relief was placed on a statutory footing in the UK (at least for Scotland) by virtue of the Intellectual Property (Enforcement, etc) Regulations 2006 which transpose the Enforcement Directive⁶⁰⁹ into local law.⁶¹⁰

⁶⁰⁶ So-called after the House of Lords decision in *Norwich Pharmacal Co v Customs & Excise Commissioners* [1974] AC 133. Now formalised in the Civil Procedure Rules 1998, SI 1988/3132, r 31.18: 'Rules 31.16 and 31.17 do not limit any power which the court may have to order (a) disclosure before proceedings have started; and (b) disclosure against a person who is not a party to proceedings.' A *Norwich Pharmacal* Order will protect the ISP from claims that it is in breach of the confidentiality and privacy agreements that it has with its customers. Craig Earnshaw and Sandeep Jadav, 'E-Mail Tracing' (2004) 15 C & L 9.

⁶⁰⁷ *Norwich Pharmacal v Customs and Excise Commissioners* [1974] AC 133, 175.

⁶⁰⁸ *Mitsui & Co Ltd v Nexen Petroleum UK Ltd* [2005] EWHC 625 (Ch) [24].

⁶⁰⁹ Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L157/45 (in short referred to as the Enforcement Directive).

⁶¹⁰ The Intellectual Property (Enforcements, etc) Regulations 2006, SI 2006/1028; Kirstin Huniar, 'The Enforcement Directive – its effects on UK Law' (2006) 28 EIPR 92-99 (with a section on *Norwich Pharmacal* Orders on p 97).

Regulation 4 of these regulations implements Article 8 of the Enforcement Directive ('Right of Information')⁶¹¹ in Scotland while no provision was deemed necessary to implement that particular obligation in England & Wales or Northern Ireland due to the existence of the House of Lords ruling in *Norwich Pharmacal v Customs and Excise Commissioners*.

In England, a *Norwich Pharmacal* order is granted at an interlocutory stage in a lawsuit while under the Enforcement Directive, the relevant information can be obtained by requesting a court order. This request does not have to be made at an interlocutory stage of the proceedings. A discovery order can be sought before an infringement action has begun as well as after. Clearly where the internet is concerned, an ISP could be viewed as facilitating a subscriber's wrongdoing, merely through the provision of access.

7.3.2 Case law featuring *Norwich Pharmacal* relief

This section will set out general principles established by the courts in respect of this form of equitable relief. While not all the case law analysed will be IPR-centric, there will be a special focus on torts (IPRs and defamation). Disclosure can be ordered where the claimant requires the disclosure of crucial information in order to bring a claim or where the claimant requires a missing piece of the information.

The rulings below are being treated in chronological order.

7.3.2.1 *Coca Cola Company v British Telecommunications plc*

⁶¹¹ The Intellectual Property (Enforcements, etc) Regulations 2006, SI 2006/1028, reg 4; Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2009 on the enforcement of intellectual property rights [2004] OJ L195/16, art 8(1)(c) provides as follows:

Member States shall ensure that, in the context of proceedings concerning an infringement of an intellectual property right and in response to a justified and proportionate request of the claimant, the competent judicial authorities may order that information on the origin and distribution networks of the goods or services which infringe an intellectual property right be provided by the infringer and/or any other person who (...) was found to be providing on a commercial scale services used in infringing activities.

*Coca Cola Company v British Telecommunications plc*⁶¹² concerned the application of the *Norwich Pharmacal* procedure in a communications environment. BT challenged a *Norwich Pharmacal* order requiring it to deliver-up one of its subscribers (mobile phone customer) details, for the purpose of proceedings relating to infringement of Coca Cola's IPRs. The court ruled that the information held by BT was critical to the successful pursuance of Coca Cola's civil rights and therefore the information had to be disclosed.⁶¹³

7.3.2.2 *Totalise plc v Motley Fool Ltd*

Totalise plc v Motley Fool Ltd.⁶¹⁴ Website operators should disclose the identity of wrongdoers (in this case, an offender posting defamatory material on a website operator's discussion board). The House of Lords emphasized that the *Norwich Pharmacal* line of authority, developed by 2001, was not restricted by Section 35 of the Data Protection Act 1998 (DPA). It remains in the court's discretion whether or not to grant a *Norwich Pharmacal* order, which depends, among other things, on the strength of the claimant's case and whether the defendant had a confidentiality policy for website users.⁶¹⁵

7.3.2.3 *Takenaka (UK) v Frankl Ltd*

*Takenaka (UK) v Frankl Ltd*⁶¹⁶ involved a defendant who had gone to considerable lengths to hide their identity. The case concerned defamatory e-mails but thanks to a series of *Norwich Pharmacal* proceedings against various ISPs, including Hotmail and CompuServe, the claimants came to the conclusion that the infringing computer was located in Turkey. The claimants were able to link that computer to the defendant.

The general principle upon which *Norwich Pharmacal* relief is founded was set out by Lord Woolf in the House of Lords in *Ashworth Hospital Authority v MGN Ltd*⁶¹⁷ where he stated as follows:

⁶¹² *Coca Cola Company v British Telecommunications plc* [1999] FSR 518.

⁶¹³ *Ibid* 523 et seq.

⁶¹⁴ *Totalise plc v Motley Fool Ltd* [2002] 1 WLR 1233.

⁶¹⁵ *Ibid* [19] et seq, [23].

⁶¹⁶ *Takenaka (UK) Ltd v Frankl* [2001] EWCA Civ 348.

⁶¹⁷ *Ashworth Hospital Authority v MGN Ltd* [2002] 1 WLR 2033.

The Norwich Pharmacal case clearly establishes that where a person, albeit innocently, and without incurring any personal liability, becomes involved in a wrongful act of another, that person thereby comes under a duty to assist the person injured by those acts by giving him any information which he is able to give by way of discovery that discloses the identity of the wrongdoer.⁶¹⁸

7.3.2.4 Mitsui & Co Ltd v Nexen Petroleum UK Ltd

Mitsui & Co Ltd v Nexen Petroleum UK Ltd:⁶¹⁹ The following conditions must be satisfied before a *Norwich Pharmacal* order can be granted: (1) a wrong must have been carried out or allegedly carried out by a wrongdoer; (2) there must be the need for the order to enable action to be brought against the wrongdoer; and (3) the person against whom the order was sought must be somehow involved in the wrongdoing so as to have facilitated it, and must be able or likely to be able to provide the information necessary to enable the wrongdoer to be sued.⁶²⁰

7.3.2.5 Grant v Google UK Ltd

Grant v Google UK Ltd⁶²¹ involved a Trust (The Individuals Self-Discovery Trust), which owned the copyright of an unpublished work entitled 'Unlock Reality'. Without the Trust's consent, an early draft of the work had been made available on the internet through an advertisement generated by the Google search engine. This advertisement led ultimately to a website at Realityunlocked.com. The Trust sought Google's assistance in the identification of the advertiser but it declined to comply, saying it could not do so, perhaps because of a perceived duty of confidentiality to its customers. Google did, however, suggest that the Trust should apply for an order requiring Google to make the requested disclosure, which it would not oppose. The Trust applied for such order and the relief sought was granted by Rimer J in the Chancery Division of the English High Court. The relief was granted because Google had become mixed up in the apparent wrongdoing of others but it was still in a position to disclose the identity of those others to the Trust.

⁶¹⁸ Ibid 2039.

⁶¹⁹ *Mitsui & Co Ltd v Nexen Petroleum UK Ltd* [2005] EWHC 625 (Ch).

⁶²⁰ Ibid [24].

⁶²¹ *Grant v Google UK Ltd* [2005] EWHC 3444 (Ch).

7.3.2.6 *Smith v ADVFN plc*

Smith v ADVFN plc.⁶²² The Court of Appeal considered the proper ambit of a *Norwich Pharmacal* order and, in particular, the coherency and quantity of the evidence supporting a *Norwich Pharmacal* order.

This case concerned alleged defamatory postings (done under cover of pseudonyms) on a bulletin board on a financial services website. In refusing the appellants request for *Norwich Pharmacal* relief, it was held unreasonable to expect the judge, in the short time available, to assess without proper guidance each and every alleged instance of defamation, given the volume and incoherence of the material which he had been expected to consider.⁶²³ In short, the court scrutinises the presentation of the evidence and there is an onus on the applicant to provide the courts with a coherent body of data from which an allegation of wrongdoing could properly be assessed.

This judgment may serve as a corrective and may reduce the tendency among judges to grant the application without proper consideration of whether the material complained of was, in fact, defamatory. The case confirms that *Norwich Pharmacal* relief applications should be used with caution. If the claimant can get the documents from another source or by other means, the court will not grant the orders and the claimant may find itself facing the third party's legal costs.

7.3.2.7 *Media C.A.T. v Adams and Others*

Media C.A.T. v Adams and Others⁶²⁴

Despite being a ruling from one of the UK's junior courts, its importance may be significantly greater than its rather humble provenance! Judge Birss considered the appropriateness of the *Norwich Pharmacal* Order and when it should be used. In short, he was quite critical of the use of NPOs as he believed that there was a lack of safeguards (governing) the use of the information obtained under NPOs. While the

⁶²² *Smith v ADVFN plc* [2008] EWCA Civ 518.

⁶²³ *Ibid* [14].

⁶²⁴ *Media C.A.T. v Adams and Others* [2011] EWPC 6.

Media C.A.T. case has not altered the rules or law on the obtaining of a NPO, it has raised a number of questions about the operation of NPOs.

The case concerned allegations of copyright infringement in the context of pornographic films. The claimants argued that the defendants had used P2P file-sharing software on the internet to carry out the infringements.

Following the grant of NPOs by Chief Master Winegarten, the names and addresses of tens of thousands of people were disclosed by ISPs. Armed with this information, ACS Law sent out speculative invoicing letters to suspected copyright infringers while Media C.A.T., through ACS Law, wrote to all those identified through the NPOs, claiming £495 for breach of copyright. The claimant and their legal advisor tried to intimidate the defendants into making payment for supposed copyright infringement even when they were not entirely sure they were pursuing the correct people. In his ruling, Birss J stated that when a NPO is made, it may well be worth considering how to manage the subsequent use of the identities disclosed.⁶²⁵ He suggested that consideration be given to the making of a Group Litigation Order under CPR ((Civil Procedure Rules)) Part 19 from the outset and the provision of a mechanism for identifying test cases at an early stage before a letter writing campaign begins.⁶²⁶

Using the example of Anton Piller orders, he also suggested the appointment of a neutral supervising solicitor whose task it would be to ensure that the NPO is not abused.⁶²⁷

This ruling represents a more critical interpretation of *Norwich Pharmacal* relief in which the presiding judge is live to the real risk of the (successful applicants) ‘beneficiaries’ under a NPO abusing the information disclosed under the order. It will be interesting to see whether Birss J’s suggestions will be accepted in the future. Indeed, they may act as a ‘brake’ on the granting of NPOs.

While *Media C.A.T.* does not alter the rules or law on the obtaining of a *Norwich Pharmacal* Order, it has certainly raised questions that need to be borne in mind by members of the judiciary when considering future applications. Potentially, the ruling

⁶²⁵ Ibid [112].

⁶²⁶ Ibid.

⁶²⁷ Ibid.

could act as a catalyst for a complete re-examination of the *Norwich Pharmacal* jurisdiction.

Following Judge Birss' suggestions, courts may well include in their orders the appointment of a supervising solicitor. Indeed, they may even go further by placing restrictions on information disclosed under *Norwich Pharmacal* Orders or even require the parties to return to the judge who made the original order so that he/she could provide directions upon use once the information has been obtained and can be considered.

7.3.2.8 Rugby Football Union v Viagogo Ltd

Rugby Football Union v Viagogo Ltd:⁶²⁸ The RFU alleged that Viagogo had permitted a large number of tickets for international rugby matches to be advertised on its website for sale at prices far above the face value of the tickets. The RFU alleged that Viagogo had become innocently involved in such wrongdoing and that the court should make a *Norwich Pharmacal* order requiring Viagogo to identify the persons advertising and selling such tickets. At first instance, Tugendhat J ruled that the court should exercise its discretion in favour of granting *Norwich Pharmacal* relief.⁶²⁹ In the Court of Appeal, Viagogo argued that the order sought involved an interference with the fundamental rights of individuals under the EU Charter of Fundamental Rights, namely Articles 7 (respect for private and family life) and 8 (protection of personal data). They also invoked Section 35, DPA 1998. In support of their argument, Viagogo relied upon two decisions of the CJEU, C-73/07 *TietosuojaValtuutettu v Satakunen Markkinaporssi Oy*⁶³⁰ and Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*.⁶³¹ The Court of Appeal affirmed Tugendhat J's decision and ruled that the disclosure was both necessary and proportionate.⁶³² Delivering the judgment, Longmore LJ concluded that the RFU had no available means of finding out the

⁶²⁸ *Rugby Football Union v Viagogo Ltd* [2011] EWCA Civ 1585.

⁶²⁹ *Ibid* [78].

⁶³⁰ Case C-73/07 *TietosuojaValtuutettu v Satakunen Markkinaporssi Oy* [2008] ECR I-9831.

⁶³¹ Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] ECR I-11063.

⁶³² *Rugby Football Union v Viagogo Ltd* [2011] EWCA Civ 1585 [79] et seq.

information it was seeking other than through Viagogo and that the making of the *Norwich Pharmacal* order was therefore necessary.⁶³³

There was a further appeal by Viagogo (in liquidation) to the Supreme Court.⁶³⁴ In the UK's highest court, Lord Kerr held that the appropriate test of proportionality under Article 8 of the Charter of Fundamental Rights of the European Union involved weighing the benefit of the information being sought by the RFU against the impact that disclosure was likely to have on the individual concerned.⁶³⁵ The court acknowledged that there should be an intense focus on the rights claimed by the individuals concerned but this was not a case where disclosure would result in oppressive or unfair treatment.⁶³⁶ The only information sought was the names and addresses of individuals who had bought and sold tickets in clear breach of the RFU's ticket policy.⁶³⁷

The Supreme Court acknowledged that in 'some limited instances', the particular circumstances affecting the individual whose personal data will be revealed on foot of a NPO may displace the interests of the applicant for the disclosure of the information.⁶³⁸ But, in the case before the court, the impact that could reasonably be apprehended by the individuals, whose personal data was being sought, was simply not of the type that could possibly offset the interests of the RFU in obtaining that information.⁶³⁹ For that reason, the court dismissed the appeal.

7.3.2.9 *Golden Eye (International) Ltd v Telefonica UK Ltd*

Golden Eye (International) Ltd v Telefonica UK Ltd.⁶⁴⁰ This was a claim by Golden Eye (International) Ltd and thirteen other claimants for a *Norwich Pharmacal* order against Telefonica UK (trading as 02). The object of the claim was to obtain disclosure

⁶³³ Ibid [79].

⁶³⁴ *Rugby Football Union v Consolidated Information Services Limited (Formerly Viagogo Limited) (In Liquidation)* [2012] UKSC 55.

⁶³⁵ Ibid [33]-[36].

⁶³⁶ Ibid [45].

⁶³⁷ Ibid [43] et seqq.

⁶³⁸ Ibid [46].

⁶³⁹ Ibid.

⁶⁴⁰ *Golden Eye (International) Ltd v Telefonica UK Ltd* [2012] EWHC 723 (Ch).

of the names and addresses of customers of O2 who allegedly committed copyright infringements through peer-to-peer files-sharing using the BitTorrent protocol. The subject-matter of the alleged infringements was pornographic films, owned by the claimants. The case raised fundamental questions as to the operation of the *Norwich Pharmacal* regime, the legitimacy of speculative invoicing, the issue of whether there is a duty of full and frank disclosure on a *Norwich Pharmacal* application⁶⁴¹ and, how to balance the rights of copyright owners and consumers.

On the issue of necessity, Arnold J held that it was plainly necessary for the information sought to be disclosed for the claimants to be able to protect their copyrights.⁶⁴² As regards the issue of proportionality, Arnold J referred to Article 3(2) of the Enforcement Directive which imposes a general obligation to consider the proportionality of remedies for the infringement of IPRs including orders for the disclosure of the identities of infringers.⁶⁴³ He went on to state that the CJEU had ruled that, when adopting measures to protect copyright owners against online infringement, national courts must strike a fair balance between the protection of IPRs guaranteed by Article 17(2) of the EU's Charter of Fundamental Rights and the protection of the fundamental rights of individuals who are affected by such measures, and in particular the rights safeguarded by Articles 7 and 8 of the EU Charter of Fundamental Rights.⁶⁴⁴ Ultimately,

⁶⁴¹ Ibid [84] et seq. Arnold J stated that it was an issue to be decided in another case, not this one. He went on to say that such a duty normally comes into play when the respondent to the application applies to set aside the order on the ground of non-compliance with that duty. It is also well established that a court may set aside an order made on a without notice application and decline to grant a fresh one if the applicant has not complied with the duty. However, at the stage of the without notice application, the court will normally assume that the applicant is complying with the duty (para [86]). Mr Justice Arnold did highlight the fact that Golden Eye had not explained to counsel for Consumer Focus why it discontinued at least two claims. This failure to explain is something that a court could and should take into account (para [88]).

⁶⁴² Ibid [114] et seq.

⁶⁴³ Ibid [116]. Arnold J also cited Case C-324/09 *L'Oreal SA v eBay International AG* [2011] ECR I-6011, paras 139-144.

⁶⁴⁴ For a good example of a national court attempting to strike a fair balance between protection of IPRs and privacy rights, see the Irish High Court ruling from 2012, *EMI Records (Ireland) Limited & Ors v The Data Protection Commissioner & Anor* [2012] IEHC 264. The context was unauthorised sharing of copyright material and legal proceedings brought against

Arnold J held that the claimants' interests in enforcing their copyright outweighed the intended defendants' interest in protecting their privacy and data protection rights and thus it was proportionate to order disclosure provided that the order and the proposed letter of claim were framed so as to properly safeguard the legitimate interests of the intended defendants and in particular the interests of intended defendants who have not in fact committed the infringements in question.⁶⁴⁵ Accordingly, he made a *Norwich Pharmacal* order in favour of Golden Eye and its exclusive licensee, Ben Dover Productions, but declined to make an order in favour of the other claimants. The Other claimants appealed the High Court's decision not to extend *Norwich Pharmacal* relief to them. They contended, before the Court of Appeal,⁶⁴⁶ that it was both illogical and inconsistent for the judge to deny the self-same relief to them merely because they had chosen to pursue their claims with the assistance of Golden Eye under arrangements which the judge had previously found to be both lawful and not part of a speculative invoicing scheme.⁶⁴⁷

Lord Justice Patten identified the reason for Arnold J's refusal to grant relief to the Other Claimants – it was, in essence, that judge's disapproval of the recovery sharing arrangements with Golden Eye. Patten LJ found Mr Justice Arnold's reasoning difficult to follow. In fact, Patten LJ's assessment was rather blunt. He reasoned that where the arrangements between Golden Eye and the Other Claimants were neither unlawful nor simply a money-making exercise designed to take advantage of the vulnerability of the subscribers (rather than a genuine attempt to protect the rights the Other Claimants), then he could see no justification for refusing relief based on a disapproval of those arrangements.⁶⁴⁸ Indeed, he found it difficult to articulate what the disapproval could be based on. Factoring in the safeguards put in place by Arnold J to protect the intended

Ireland's largest ISP, Eircom, by some of Ireland's record companies. The relevant part of the ruling is para [8.10] where Charleton J considers the 'proportionality of an injunctive remedy' in the context of 'the mischief of the improper use of intellectual property online'.

⁶⁴⁵ *Golden Eye (International) Ltd v Telefonica UK Ltd* [2012] EWHC 723 (Ch) [145].

⁶⁴⁶ For a detailed analysis of the Court of Appeal ruling in *Golden Eye*, see Mark Hyland, 'The seductive interface between adult entertainment and *Norwich Pharmacal* relief' (2013) 18 *Comms L* 56-59.

⁶⁴⁷ *Golden Eye (International) Ltd v Telefonica UK Ltd* [2012] EWCA Civ 1740 [25].

⁶⁴⁸ *Ibid* [28].

defendants, Patten LJ considered that the balance had been tipped in favour of making the order.⁶⁴⁹ He therefore allowed the appeal.

7.3.3 *Digital Economy Act 2010*

Theoretically, under the DEA 2010, there are a number of provisions that safeguard the position of copyright owners. They include Section 3 (obligation on ISPs to notify subscribers of reported infringements), Section 4 (obligation on ISPs to provide infringement lists to copyright owners), Section 9 (Obligations on ISPs to take technical measures against subscribers for the purpose of preventing or reducing infringement of copyright by) and Section 10 (Obligations to limit internet access). However, in reality, given the serious delays in the implementation of the DEA 2010,⁶⁵⁰ these provisions are increasingly being viewed as ineffective.

It is now likely that the first warning letters from ISPs to copyright infringers (under Section 3 of the DEA 2010) will only go out in 2016 at the earliest and, with a general election coming up in the UK next year, there is no certainty that the next government will demonstrate as much resolve in tackling online copyright infringement.

From a rightholder's perspective, the DEA 2010 was further weakened by the government's announcement in June 2012 to repeal sections 17 and 18 of the Act, referring in the process to the Ofcom report⁶⁵¹ and the fact that rightholders have successfully used Section 97A, CDPA 1988 to secure website blocks (e.g. Newzbin2 and Pirate Bay).⁶⁵² Under Section 17, the Secretary of State for Culture, Media and Sport has the power to make provision about blocking injunctions which would prevent access to locations on the internet which are being used or likely to be used in connection with copyright infringement.

⁶⁴⁹ Ibid [29].

⁶⁵⁰ BBC, 'UK Piracy warning letters delayed until 2015' (*BBC News Technology*, 6 June 2013) <<http://www.bbc.co.uk/news/technology-22796723>> accessed 8 May 2014.

⁶⁵¹ Ofcom, "'Site Blocking'" to reduce online copyright infringement, A review of sections 17 and 18 of the Digital Economy Act' (27 May 2010) <<http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf>> accessed 8 May 2014.

⁶⁵² Department for Culture, Media & Sport, 'Next steps to tackle internet piracy' (26 June 2012) <<https://www.gov.uk/government/news/next-steps-to-tackle-internet-piracy>> accessed 3 June 2014; See para 7.3.5. (below) for treatment of web-blocking cases. .

7.3.4 Technical Measures Legislation in France and the Republic of Ireland

7.3.4.1 France

The UK was not the only EU Member State to introduce technical measures legislation, often colloquially termed ‘three strikes legislation’. In October 2009, the HADOPI law was passed in France. The law created a new independent public body - the Haute Autorité pour la Diffusion des œuvres et la Protection des droits d'auteur sur Internet (HADOPI) (in English, the High Authority for the Distribution of Works and the Protection of Rights on the Internet). During the first three years of the HADOPI’s existence, only 14 cases were forwarded to prosecutors. Of those, only one resulted in a conviction carrying a financial penalty.⁶⁵³ The new body has attracted considerable criticism, principally along the lines of whether it is good value for money.

Little wonder then that the body recently had its budget slashed and that rumours circulate that its role and powers may soon be transferred to the Conseil Supérieur de l’Audiovisuel (Audiovisual High Council).⁶⁵⁴

7.3.4.2 The Republic of Ireland

The Republic of Ireland introduced a voluntary three-strikes policy (the Graduated Response Protocol) in August 2010 but not all ISPs have signed up to this protocol. In 2012, the protocol survived a challenge from the Irish Data Protection Commissioner.⁶⁵⁵ Recent truculence by UPC Communications, Ireland’s second largest ISP, raised the ire of Mr Justice Peter Kelly. UPC’s reluctance to implement a graduated response similar to that being operated by Eircom, the Republic’s largest ISP, resulted in Mr Justice

⁶⁵³ Andrew Murray, *Information Technology Law, The Law and Society* (2nd, OUP 2013) 284.

⁶⁵⁴ Laura Bérard, ‘Intellectual Property Rights Protection on the Internet in France: The End of Hadopi?’ (*LSE*, 29 January 2014) <<http://blogs.lse.ac.uk/mediapolicyproject/2014/01/29/intellectual-property-rights-protection-on-the-internet-in-france-the-end-of-hadopi>> accessed 3 June 2014.

⁶⁵⁵ *EMI Records (Ireland) Ltd and ors v The Data Protection Commissioner & Anor* [2012] IEHC 264.

Peter Kelly deciding on 10th February to fast-track in the Commercial Court an action being brought by three of Ireland's music companies against UPC Communications.⁶⁵⁶

7.3.5 Section 97A CDPA 1988 and Blocking of Websites

Ever since the 2011 High Court ruling in *Twentieth Century Fox v British Telecommunications*,⁶⁵⁷ there has been a gradual judicial expansion in terms of Section 97A CDPA 1988 and this, despite the restrictive CJEU ruling in *Scarlet Extended SA v SABAM*.⁶⁵⁸ This judicial expansionism, combined with Arnold J's bullish approach to Article 15(1) of the E-Commerce Directive,⁶⁵⁹ effectively means that the DEA 2010 is being bypassed.

I shall now examine the six High Court cases on web-blocking. I shall deal with them in chronological order, starting with *Twentieth Century Fox v British Telecommunications (Newzbin 2)*.⁶⁶⁰ In each case, the remedy sought by copyright owners has been a blocking order imposed against an ISP and requiring it to block access to one or more copyright infringing websites. The latest ruling in this line of authorities - *Paramount Home Entertainment International Ltd v British Sky Broadcasting*⁶⁶¹ – was handed down on 13 November 2013. It involved the blocking of two websites - TubePlus and SolarMovie, both of which were providing access via an online database to a large number of television programmes and films without the rightholder's authorisation.

⁶⁵⁶ Mary Carolan, 'Legal action to stop UPC users downloading illegally' (*The Irish Times*, 10 February 2014) <<http://www.irishtimes.com/news/crime-and-law/courts/legal-action-to-stop-upc-users-downloading-illegally-1.1686474>> accessed 8 May 2014.

⁶⁵⁷ *Twentieth Century Fox v British Telecommunications* [2011] EWHC 1981 (Ch).

⁶⁵⁸ Case C-70/10 *Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs (SABAM)* [2011] ECR I-11959. In short, in *Scarlet Extended*, the CJEU held that ISPs could not be required to filter and block access by its customers to files containing infringing copies of musical works as such a requirement would amount to a general monitoring obligation, which is explicitly prohibited by Article 15(1) of the E-Commerce Directive.

⁶⁵⁹ Article 15(1) of the E-Commerce Directive obliges Member States not to impose a general monitoring obligation on ISPs in terms of information which they transmit or store while providing e-commerce services.

⁶⁶⁰ *Twentieth Century Fox v British Telecommunications plc* [2011] EWHC 1981 (Ch).

⁶⁶¹ *Paramount Home Entertainment International Ltd v British Sky Broadcasting* [2013] EWHC 3479 (Ch).

All the blocking orders are granted under Section 97A, CDPA 1988 which empowers the High Court to grant injunctions against any service provider which has actual knowledge of a person using its services to infringe copyright.⁶⁶²

7.3.5.1 *Twentieth Century Fox v British Telecommunications (Newzbin 2)*

In *Twentieth Century Fox v British Telecommunications plc*⁶⁶³ ((Newzbin 2)), BT was ordered by the High Court to block access to www.newzbin.com using its 'Cleanfeed' system, a system usually used to block access to child sexual abuse material on the internet (in collaboration with the Internet Watch Foundation). The Newzbin website (which has since closed down) acted as a search engine directed to Usenet, a platform for posting and retrieving large binary content such as films, TV shows etc., much of which was infringing material.

In granting the order against BT, Arnold J held that in terms of the knowledge requirement what had to be shown was that the 'service provider has actual knowledge of one or more persons using its service to infringe copyright' as opposed to 'actual knowledge of a specific infringement of a specific copyright work by a specific individual'.⁶⁶⁴

This ruling is significant as it is the first time that a site-blocking order was made by the English courts. Its precedential value has been proven over the last three years as copyright owners now seem more inclined to go the Section 97A route than the *Norwich Pharmacal* route.

7.3.5.2 *Twentieth Century Fox v British Telecommunications (No 2)*

The form of the order (against BT) is set out in *Twentieth Century Fox v BT (No 2)*⁶⁶⁵. This ruling also contains an interesting debate on the differences between Section 97A, CDPA 1988 and *Norwich Pharmacal* orders.

⁶⁶² S 97A, CDPA 1988 implements Article 8(3) of Directive 2001/29/EC into UK law. Article 8(3) provides that 'Member States shall ensure that rightsholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right'.

⁶⁶³ *Twentieth Century Fox v British Telecom* [2011] EWHC 1981 (Ch).

⁶⁶⁴ *Ibid* [148].

⁶⁶⁵ *Twentieth Century Fox v BT (No 2)* [2011] EWHC 2714 (Ch).

By way of the order, BT was required within 14 days to adopt a prescribed technical means to block or attempt to block access by its customers to Newzbin2 (accessible at www.newzbin.com), its domains and sub-domains and any other IP address or URL whose sole/predominant purpose was to enable or facilitate access to the Newzbin2 website. The prescribed technical means included

- (i) IP address re-routing in respect of each and every IP address from which the said website operates (this could be achieved using Cleanfeed), and
- (ii) DPI-based URL blocking utilising at least summary analysis in respect of each and every URL available at the said website and its domains and sub-domains.⁶⁶⁶

The analysis of the distinctions between an order under Article 8(3) and a *Norwich Pharmacal* Order occur at paragraphs 27-31 of the ruling. The two most important distinctions drawn by counsel for the applicants (and accepted by Arnold J) are, firstly, that Article 8(3) confers on rightholders a legal right to the substantive remedy of a final injunction whereas applicants for *Norwich Pharmacal* Orders have no such right where the respondent is innocent of wrongdoing.

Secondly, a *Norwich Pharmacal* application is a preparatory step for the bringing of proceedings against the wrongdoer. In contrast, an order under Article 8(3) is not preparatory to proceedings (or other steps) against the infringer but may well follow such proceedings.

7.3.5.3 Dramatico Entertainment Limited v British Sky Broadcasting Limited (2 rulings; February and May 2012)

In the two rulings of 2012, both involving Dramatico Entertainment as claimant,⁶⁶⁷ the targeted (offending) website was The Pirate Bay. On 27 April 2012, Arnold J made an order under Section 97A, CDPA 1988 requiring five of the six largest UK ISPs to block access to The Pirate Bay website, self-described as ‘the world’s largest BitTorrent

⁶⁶⁶ Ibid [56].

⁶⁶⁷ *Dramatico Entertainment Limited v British Sky Broadcasting Limited* [2012] EWHC 268 (Ch) [20 February 2012] and *Dramatico Entertainment Limited v British Sky Broadcasting Limited* [2012] EWHC 1152 (Ch) [2 May 2012].

tracker'.⁶⁶⁸ The more interesting of the two related rulings is that on the merits, handed down on 20th February 2012.

Two of the more interesting components of the February ruling relate to the restricted act of communication to the public and, the notions of authorisation/joint tortfeasance.

In considering whether users of The Pirate Bay communicated such recordings to the public, Arnold J posed two questions. Firstly, do the users communicate the recordings by electronic transmission? He answered that in the affirmative and added that this was done in such a way as to allow members of the public access the recordings from a place and at a time individually chosen by them (within the meaning of section 20(2)(b), CDPA 1988). Mr Justice Arnold added that in any event, it is clear from the CJEU's ruling in *Football Association Premier League Ltd v QC Leisure*⁶⁶⁹ (analysed at para. 3.6.1.) that the concept of communication must be construed broadly.⁶⁷⁰

The second question was: do the Pirate Bay users communicate the recordings to a *new* public, that is to say a public which was not taken into account by the rightholders when authorising the distribution of the recordings, in essence, applying the test laid down by the CJEU in a line of cases starting with *Sociedad General de Autores v Editores de España (SGAE)*.⁶⁷¹ Once again, Arnold J answered in the affirmative as, in his judgement, copies of sound recordings were made available to users who had not purchased them from an authorised source.⁶⁷²

As for the notion of authorisation, Mr Justice Arnold referred to expert evidence adduced by John Hodge, BPI's Head of Internet Investigations, in which the functions

⁶⁶⁸ Hogan Lovells and Alastair Shaw, 'Pirate Bay watch: UK ISPs ordered to block The Pirate Bay' (ACC, 20 July 2012) <<http://www.lexology.com/library/detail.aspx?g=29d6e1b2-2c1a-40b8-92f9-0e53a166dd93>> accessed 7 May 2014.

⁶⁶⁹ Cases C-403/08 and C-429/08 *Football Association Premier League Ltd v QC Leisure; Karen Murphy v Media Protection Services Ltd* [2011] ECR I-9083, para 93.

⁶⁷⁰ *Dramatico Entertainment Limited v British Sky Broadcasting Limited* [2012] EWHC 268 (Ch) [69].

⁶⁷¹ Case C-306/05 *Sociedad General de Autores v Editores de España (SGAE)* [2006] ECR I-11519.

⁶⁷² *Dramatico Entertainment Limited v British Sky Broadcasting Limited* [2012] EWHC 268 (Ch) [70].

and features of The Pirate Bay website were highlighted.⁶⁷³ He held that the operators of the Pirate Bay did authorise its users' infringing acts of copying and communication to the public. This was done by going 'far beyond merely enabling or assisting'. In Arnold J's view, they sanctioned, approved and countenanced the infringements of copyright committed by its users.⁶⁷⁴

As for the issue of joint tortfeasance, having considered Kitchin J's analysis of the law in *Twentieth Century Fox v Newzbin*, Arnold J was of the view that the operators of The Pirate Bay induced, incited or persuaded its users to commit infringements of copyright.⁶⁷⁵ Moreover, they and the users acted pursuant to a common design to infringe. In short, the Hon Mr Justice Arnold found both parties to be jointly liable for the infringements committed by users.⁶⁷⁶

The *Newzbin2* and *Dramatico* rulings demonstrate that rightholders (or their representatives) will not hesitate to invoke Section 97A, CDPA 1988 particularly if the whereabouts of the operator of an offending/authorising website is not known (eg The Pirate Bay). Cynically, one could argue that they have no option given that the anti-piracy measures contained in the 2010 Digital Economy Act have yet to be implemented. Following *Dramatico*, it is becoming increasingly clear that ISPs have considerable responsibility in the whole area of copyright infringement by their users – it behoves them to take a more active role in infringement prevention.

7.3.5.4 EMI Records Limited v British Sky Broadcasting Limited (2013)⁶⁷⁷

Like the previous cases, the claimants here are record companies claiming on their own behalf and in a representative capacity on behalf of other members of the British Phonographic Industry (BPI) and the Phonographic Performance Limited (PPL). The defendants are the six main ISPs in the UK. The claimants sought an injunction against the defendants pursuant to Section 97A, CDPA 1988 to block or at least impede access

⁶⁷³ Ibid [75].

⁶⁷⁴ Ibid [81].

⁶⁷⁵ Ibid [83].

⁶⁷⁶ Ibid.

⁶⁷⁷ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch).

by their customers to three P2P file-sharing websites called KAT, H33T and Fenopy (hereafter, the websites). As well as operating as BitTorrent indexing websites, the three websites also offered so-called magnet links, which are a different means of using the relevant torrent file to obtain the content.

One aspect of the application that is revealing is the list of entities which supported the claimants' application, namely, the MCPS-PRS Alliance Ltd, the Motion Picture Association, the Producers Alliance for Cinema and Television, the Association for UK interactive Entertainment and the Publishers' Association Ltd. The industries represented are most likely setting down a marker as to their possible future reliance on Section 97A!

A significant portion of the ruling is given over to the principle of proportionality. Adverting to his ruling in *Golden Eye (International) Ltd v Telefonica UK Ltd*,⁶⁷⁸ Mr Justice Arnold re-stated the two reasons why it is necessary to consider the proportionality of orders in the field of IP Law. Firstly, Article 3(2) of Directive 2004/48/EC (the Enforcement Directive) imposes a general obligation to consider the proportionality of remedies for the infringement of IPRs. Secondly, the CJEU has held that, when adopting measures to protect copyright owners against online infringement, national courts must strike a fair balance between the protection of IPRs guaranteed by Article 17(2) of the Charter of Fundamental Rights of the European Union and the protection of the fundamental rights of individuals who are affected by such measures and in particular the rights safeguarded by the applicable articles of the Charter.⁶⁷⁹ Arnold J's approach to considering proportionality (as set out in *Golden Eye*⁶⁸⁰ at [117]) is recapitulated as are the relevant legal instruments (and relevant provisions) under which both the copyright owner and users of infringing material derive rights.⁶⁸¹

⁶⁷⁸ *Golden Eye (International) Ltd v Telefonica UK Ltd* [2012] EWHC 723 (Ch).

⁶⁷⁹ See Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-271, paras 61-68; Case C-70/10 *Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs (SABAM)* [2011] ECR I-11959, paras 42-46, 50-53; and Case C-360/10 *Société belge des auteurs compositeurs et éditeurs (SABAM) v Netlog NV* [2012] 2 CMLR 18, paras 41-51.

⁶⁸⁰ *Golden Eye (International) Ltd v Telefonica UK Ltd* [2012] EWHC 723 (Ch).

⁶⁸¹ *EMI Records Limited v British Sky Broadcasting Limited* [2013] EWHC 379 (Ch) [92].

Towards the end of his judgment, Arnold J addressed some practical considerations of the website blocking jurisdiction/regime. He stated that the proportionality of a blocking order is bound to be a context sensitive question and that the English High Court does not make such orders without a thorough consideration of whether it is appropriate to make an order in the light of the specific facts of each case.⁶⁸² Interestingly, Mr Justice Arnold is of the view that a blocking order is justified even if it only prevents access by a minority of users.⁶⁸³ He believes the efficacy of the orders is linked to the form that they take⁶⁸⁴ while the evidence in his view indicates that the blocking orders are reasonably effective. The proof of this is the order made in Italy with regard to The Pirate Bay (referred to in *Twentieth Century Fox v British Telecommunications* at [197]) which resulted in a 73% reduction in audience accessing The Pirate Bay in Italy and a 96% reduction in page views.⁶⁸⁵

One interesting part of this decision is the pragmatic approach/attitude of Mr Justice Arnold where the specific facts of the case are a determinant and blocking orders are viewed as a real possibility even if they will ‘only’ affect a minority of the users of the relevant website. Allusion to percentage reduction in access to offending websites, falling website rankings (compiled by Alexa, the Web information company), and page views creates hard data which is difficult to refute.⁶⁸⁶

7.3.5.5 The Football Association Premier League v British Sky Broadcasting Limited

This is a significant ruling since it is the first time in the UK that a site-blocking order under s 97A, CDPA 1988 has been granted in respect of streamed content rather than file-sharing websites. The English High Court granted an injunction requiring the 6 largest UK ISPs to block end-user access to the First Row Sports website, an indexing and aggregation portal, which provides unauthorised streams to live sports events including Premier League football matches.

⁶⁸² Ibid [100].

⁶⁸³ Ibid [104].

⁶⁸⁴ Ibid [105].

⁶⁸⁵ Ibid [106].

⁶⁸⁶ Ibid.

Intriguingly, the relevant website was hosted in Sweden and the alleged communications to the public originated from a host server in that country. Therefore, in order to establish the English High Court's jurisdiction, it was necessary to show that the operators of FirstRow intended to target the public in the UK.

FAPL relied on the following matters as evidencing such an intention:

- i. The website was an English language website
- ii. The advertising on FirstRow included adverts for companies located in the UK and products consumed in the UK
- iii. FirstRow provides access to a large number of competitions which are extremely popular with UK audiences. In particular, the amount of Premier League content on the website is up to 11% whilst a Premier League match is being played
- iv. FirstRow is a very popular website in the UK
- v. Between 12% and 13.7% of the worldwide traffic to the site comes from the UK
- vi. FirstRow is discussed on internet blogs and forums, where a significant proportion of the internet traffic to those blogs/forums comes from the UK.⁶⁸⁷

Mr Justice Arnold accepted that those matters evidenced an intention to target the public in the UK and that there was a communication to the public in the UK. He was also satisfied that FirstRow communicated FAPL's copyright works to the public in the UK and thereby infringed FAPL's copyrights in those works.

Another key element of the ruling concerned the principle of proportionality. FAPL put forward 5 reasons why the orders sought would be proportionate and Arnold J was satisfied by these reasons. The five reasons are as follows:

- As between FAPL and the defendants, the defendants did not oppose the making of the orders and the terms of the orders have been agreed between FAPL and the defendants. In addition, the costs to the defendants of implementation were modest and proportionate

⁶⁸⁷ *The Football Association Premier League v British Sky Broadcasting Limited* [2013] EWHC 2058 (Ch) [45].

- The orders are necessary to protect the copyrights of FAPL and the supporting rightholders, which are being infringed on a large scale. Given the difficulty of identifying let alone bringing proceedings against the operators of FirstRow, no other effective remedy was open to FAPL in the jurisdiction of England & Wales.
- The orders are also necessary or at least desirable in order to protect the sporting objectives which lie behind the Closed Period⁶⁸⁸ and, in that sense, are in the public interest.
- While FirstRow features international content some of which may not be protected by copyright or may be licensed, the vast bulk of the content which is likely to be of interest to UK users infringes the rights of FAPL and the supporting rightholders.
- The orders are narrow and targeted ones, and they contain safeguards in the event of any change of circumstances. While they are unlikely to be completely efficacious, since some users will be able to circumvent the technical measures which the orders require the Defendants to adopt, it is likely that they will be reasonably effective. The orders require IP address blocking of the IP address for FirstRow's domain name firstrow1.eu but FAPL's evidence is that this will not result in over-blocking since that IP address is not shared.⁶⁸⁹

Arnold J went on to state that the interests of FAPL and the supporting rightholders in enforcing their copyrights clearly outweighed the rights of the users of the websites under Article 11 of the Charter of Fundamental Rights of the European Union⁶⁹⁰ (the

⁶⁸⁸ The notion of 'Closed Period' is explained in para [9] of the judgment. It refers to a two and a half hour period each week during which the broadcasting of football matches is prohibited. The purpose of this is to encourage attendance at football matches and support the sport of football. Article 48 of the Statutes of UEFA provides for the Closed Period and, in the UK, the Football Association has designated 2.45pm to 5.15pm on Saturdays as the Closed Period in England.

⁶⁸⁹ *The Football Association Premier League v British Sky Broadcasting Limited* [2013] EWHC 2058 (Ch) [55] et seq.

⁶⁹⁰ This is the freedom of expression provision. Article 11(1) states as follows:

Charter), who could have obtained the copyright works from lawful sources. They even more clearly outweighed the Article 11 rights of the operators of the websites who were profiting from infringement on a large scale. Lastly, they also outweighed the defendants' Article 11 rights to the extent that they were engaged.

The significance of this ruling is linked to the fact that it breaks new ground. Previously, s 97A site-blocking orders were dominated by claimants in the music and film sectors whose rights had been undermined by illegal peer-to-peer file sharing activities. This judgment demonstrates that the s 97A remedy is also available to broadcasters of sports events who are trying to tackle unauthorised streaming of their broadcasts. The case suggests that section 97A orders will be available to an ever expanding group of rightholders though it imposes even heavier responsibilities on ISPs who are increasingly relied on to prevent piracy.

7.3.5.6 Paramount Home Entertainment v British Sky Broadcasting

The latest website-blocking ruling concerned two websites located at www.solarmovie.so and www.tubeplus.me. Both websites provided access to streams of a large range of unauthorised films and TV programmes. The mode of operation of the websites is broadly similar to that of the FirstRow website described in *Football Association Premier League v British Sky* (at [14] –[19]). Like the FirstRow website, the relevant websites do not host the content in question. Rather, they ensure that the content is comprehensively categorised, referenced, moderated and searchable.

Users who wish to access content via one of the websites are provided with a number of links. Clicking on a link enables the user to view a stream of the chosen content on an embedded player.

One novel and helpful aspect of this ruling is that Arnold J sets out the series of nine CJEU judgments⁶⁹¹ in which that court considered the concept of communication to the

Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.

⁶⁹¹ See *Paramount Home Entertainment v British Sky Broadcasting Limited* [2013] EWHC 3479 (Ch) [11]. Starting with Case C-306/05 *Sociedad General de Autores y Editores de España*

public along with 18 principles (relating to the exclusive right) which have been established by the CJEU.⁶⁹²

Arnold J acknowledged that there were three references pending before the CJEU which bore upon the issues in *Paramount*.⁶⁹³ In two of the cases, the referring courts were posing a similar question, i.e. if someone other than the copyright owner supplies a clickable link to a copyright work, does that constitute communication to the public within the meaning of Article 3(1) of Directive 2001/29/EC? The third case, *BestWater International*, was slightly more complex as it involved both linking and framing, with Arnold J speculating that an embedded stream (rather than downloading) was used to display the copyright film on the defendants' respective websites.

Interestingly, the three references to the CJEU (in particular, *Svensson*) have acted as a catalyst for academic debate on the subject of hyperlinking and communication to the public.⁶⁹⁴ Such debate includes an Opinion (published February 2013) from the European Copyright Society⁶⁹⁵ and a Report and Opinion (published September 2013) adopted by the Executive Committee of the Association Littéraire et Artistique Internationale.⁶⁹⁶

(*SGAE*) v *Rafael Hoteles SA* [2006] ECR I-11519 and running right up to the 2013 ruling in Case C-607/11 *ITV Broadcasting Ltd v TVCatchup Ltd* [2013] 3 CMLR 1.

⁶⁹² *Paramount Home Entertainment v British Sky Broadcasting Limited* [2013] EWHC 3479 (Ch) [12].

⁶⁹³ They are: Case C-466/12 *Svensson v Retriever Sverige AB* (ECJ (Fourth Chamber) 13 February 2014); Case C-279/13 *C More Entertainment AB v Sandberg* (Request for a preliminary ruling from the Högsta domstolen (Sweden) 22 May 2013); and Case C-348/13 *BestWater International GmbH v Mebes, Potsch* (Request for a preliminary ruling from the Bundesgerichtshof (Germany) 25 June 2013).

⁶⁹⁴ *Paramount Home Entertainment v British Sky Broadcasting Limited* [2013] EWHC 3479 (Ch) [29].

⁶⁹⁵ Lionel Bently, et al, 'Opinion on The Reference to the CJEU in Case C-466/12 *Svensson*' (*European Copyright Society*, 15 February 2013) <file://fs-home-l/home-009/sop01b/Windows_Data/Downloads/SSRN-id2220326.pdf> accessed 7 May 2014.

⁶⁹⁶ ALAI, 'Report and Opinion on the making available and communication to the public in the internet environment – focus on linking techniques on the Internet' (16 September 2013)

In the final analysis, Mr Justice Arnold found that there had been a communication to the public by UK users of the websites. But, he came to that conclusion by looking at the combined effect of provision of hyperlinks and the uploading of content to the host site by users. Together, these two acts amounted to communication to the public.

Adopting the same approach to the assessment of proportionality as taken in *EMI v British Sky Broadcasting*, Arnold J found that the orders sought by the claimants were proportionate and, accordingly, made the blocking orders.

Of the blocking cases, Paramount Home Entertainment is the first to analyse whether a clickable link constitutes a communication to the public. Arnold J's circumspect approach to this issue may not, however, be the final word as the CJEU has yet to rule on the three referred cases. It is also interesting to observe the gradual evolution in the blocking case-law, initially featuring BitTorrent and peer-to-peer file-sharing as the means of infringement, but, more recently featuring illegally streamed content.

From the rightholder's viewpoint, the 'tactic' of blocking the infringing website is a more practical and straightforward solution than reliance on a *Norwich Pharmacal* Order. As a *Norwich Pharmacal* Order only constitutes a preparatory step, the successful applicant (the prejudiced rightholder) must commence a fresh set of proceedings once he is armed with the relevant information (subscriber's name, address etc.) from the ISP. More compellingly, a website like The Pirate Bay attracts a very large number of users. An attempt to identify all the users using the *Norwich Pharmacal* route, while probably feasible, would be a very costly exercise. The next step – that of serving them all – might be deemed wholly disproportionate by some judges. All in all, the blocking of a copyright infringing website short circuits matters considerably for the rightholder and with an ever-expanding series of Section 97A precedents, it is difficult to see why one might opt for *Norwich Pharmacal* relief nowadays (unless of course there were evidential difficulties in terms of proving actual knowledge on the part of the ISP).

<<http://www.alai.org/assets/files/resolutions/making-available-right-report-opinion.pdf>>
accessed 7 May 2014.

7.3.5.7 Overblocking

Website blocking can also be dangerous because it brings with it significant risks of accidental 'over-blocking', the possible degradation of internet service, and it may lead to the wider, everyday use of encryption and avoidance measures. Website blocking is not always conducive to the building of vibrant digital markets but, with the warnings and data-throttling provisions in the DEA 2010 in abeyance, prejudiced rightholders may be more than happy to rely on section 97A CDPA 1988. There is quite a good discussion in the *Newzbin2* ruling⁶⁹⁷ as to the appropriate level of blocking. In short, Arnold J was open to the idea of granting a blocking order that 'should permit the Studios (the rightholders) to notify additional IP addresses and/or URLs to BT in future in order for those to be subject to the same blocking measures as *www.newzbin.com*' (para 10 of the ruling). But, the risk then exists that more websites than absolutely necessary may be blocked. Counsel for BT had argued that each additional blocking should be subject to a separate judicial determination (para 11 of the ruling).

7.3.6 The Second Facilitative Element – Geolocation Technology

As mentioned earlier in this chapter, the second facilitative element in identifying the defendant copyright infringer is technological in character, more precisely, geolocation technology.

Geolocation technology constitutes one of those technical developments the aim of which is to place geographical borders on the internet.⁶⁹⁸ From a conflicts perspective, it is a happy coincidence that this important technical advance coincides with the harmonisation of private international law at EU level. These technological advancements were frequently motivated by perceived business advantages. For example, if a website operator could see where access-seekers are located, suitable advertisement (from a cultural and linguistic perspective) could be specifically targeted at those individuals. Other perceived advantages might flow in terms of ensuring regulatory compliance, spam minimisation, reducing fraud risk and keeping licensed

⁶⁹⁷ *Twentieth Century Fox Film Corporation v British Telecommunications plc* [2011] EWHC 2714 (Ch) [10] et seqq.

⁶⁹⁸ In Lawrence Lessig, *Code and Other Laws of Cyberspace* (1st edn, Basic Books 1999) the author argues that the internet is being regulated both through law and technical developments.

content within geographical boundaries. Governments should, rationally speaking, welcome technology which facilitates the erection of geographical borders on the internet as such borders might stem the currently overly-wide extraterritorial jurisdiction claims.⁶⁹⁹

I shall now outline some of the uses that geolocation technology can be put to.

7.3.7 The Various Uses of Geolocation

After its initial use in the advertising sector, geolocation technology began to be employed by those who were attempting to comply with territorially-defined regulation. Regulation continues to be territorial in nature even in the field of copyright which is quite well harmonised internationally. Geolocation assists with the tailoring of accessibility of content on the internet to the requirements and limitations of individual countries. Some website operators use geolocation technology to comply with various regulatory requirements. For instance, Microsoft deployed geolocation tools 'to comply with US regulations prohibiting the export of strong encryption Web browser software'.⁷⁰⁰ Copyright licences too will have a strongly territorial dimension as the licensed material will only be permitted to be used in a specified geographic territory.

7.3.8 Geolocation as an enforcement tool

In reality, geolocation technology serves multiple purposes to include, for example, compliance with copyright licensing issues, the implementation of differential pricing, the localisation of advertising and internet searching. Increasingly, geolocation is used by governmental bodies as an enforcement tool in a bid to force internet actors to comply with regulatory decisions and court orders.⁷⁰¹ For example, in Italy, an operator applying for an online gaming licence is required to confirm during the application

⁶⁹⁹ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 396 et seq.

⁷⁰⁰ Michael Geist, 'Cyberlaw 2.0' (2003) 44 BCL Rev 323, 334.

⁷⁰¹ Marketa Trimble, 'The Future of Cybertravel: Legal Implications of the Evasion of Geolocation' (2012) 22 Fordham Intell Prop Media & Ent LJ 567, 589.

process which geolocation technology it intends using.⁷⁰² By deploying geolocation tools, the website operator will be able to identify the geographical origin of the individual attempting to access its gaming website. Accordingly, individuals accessing the website from Italy will be prevented from accessing non-authorised sites managed by the same operator.⁷⁰³ Similarly, in America, the US Department of Justice made it a condition of its agreement with PokerStars, an online gaming company operating from the Isle of Man, that the company utilise geographic blocking technology relating to IP addresses. In Germany, several courts have unequivocally accepted geolocation as ‘a viable and technically feasible method of determining website visitors’ locations⁷⁰⁴ and ordered online gaming operators to utilise geolocation tools to limit access to certain content from particular German states.

While Italy continues to expand the types of online gaming permitted in the country, the experience and lessons of the Italian system are being closely watched by many countries considering regulating online gaming for the first time. For example, France has studied Italy's model and has developed a similar system which it is hoping to bring on stream soon. As more and more jurisdictions learn from Italy's experience, it is likely that some form of geolocation component will become a necessary part of newly regulated online gaming markets.

7.3.9 Ensuring compliance with territorially-limited copyright laws

Geolocation technology also has a valuable part to play in terms of ensuring compliance with territorially-limited copyright laws. For example, a website operator may secure a

⁷⁰² Neustar, ‘IP Geolocation Can Ensure Compliance with New iGaming Regulations’ <http://www.neustar.biz/resources/whitepapers/ensure-uigea-compliance-whitepaper#.U030lv1_s3I> accessed 16 April 2014 (Neustar was formerly called Quova).

⁷⁰³ A hypothetical example might be as follows: an operator with a global brand and website called www.tournament.poker.com would be required to have geolocation technology in place to prevent access by players located in Italy. In contrast, a licensed site www.tournamentpoker.it would be accessible to players located in Italy.

⁷⁰⁴ See OVG Nordrhein-Westfalen [Higher Administrative Court] 02.07.2010, 13 B 646/10, [36] (the decision refers at para [37] to other German cases in which the German courts agreed that geolocation may be used to comply with their territorially-limited decisions), See generally Marketa Trimble, ‘The Future of Cybertravel: Legal Implications of the Evasion of Geolocation’ (2012) 22 Fordham Intell-Prop Media & Ent LJ 567, 590 (and fn 89).

licence for certain copyright content, but said licence may be restricted to one country or a limited number of countries. These geographically restricted licences may be preferred over a worldwide licence for a number of reasons. Firstly, the licensee might not have the necessary financial resources to pay for worldwide rights.⁷⁰⁵ Secondly, the licensor may decide not to license content in certain markets if the licensor plans to launch a country-specific version of the same content and does not want competition from foreign versions.⁷⁰⁶ Thirdly, the licensor may wish to implement a strategy for releasing the work in different countries in various media at various times.⁷⁰⁷ Lastly, copyright in a particular work might not be held by the same right-holder in all countries, and as a result there might be high transaction costs associated with locating all of the right-holders and negotiating licences with all of them, and right-holders in some countries might simply not agree to a licence.⁷⁰⁸

Given the territorially delimited nature of copyright licences, website operators and other licensees use geolocation technology to limit access to licensed content to users located only in the countries for which they have secured a licence.

The key issue really is whether geolocation tools (designed to prevent access to or certain uses of a copyright work) can be considered a technological protection measure (TPM). TPMs are described somewhat matter of factly in the Information Society Directive as ‘effective technological measures’.⁷⁰⁹ The same phrase (‘effective technological measures’) is also used in the relevant UK legal provision, i.e. Section 296ZA of the CDPA 1988.

What becomes determinative then is whether the geolocation tools meet the required standard of effectiveness. In the UK, a measure is considered ‘effective’ if it ‘achieves the intended protection’ by providing the copyright owner control of the use of the work ‘through...an access control or protection process...[or] a copy control mechanism.’⁷¹⁰ Trimble, referring to the German Copyright Act of 9th September 1965 (as amended),

⁷⁰⁵ Marketa Trimble, ‘The Future of Cybertravel: Legal Implications of the Evasion of Geolocation’(2012) 22 Fordham Intell Prop Media & Ent LJ 567, 611.

⁷⁰⁶ Ibid.

⁷⁰⁷ Ibid.

⁷⁰⁸ Ibid.

⁷⁰⁹ InfoSoc Directive, art 6(1).

⁷¹⁰ CDPA 1988, s 296ZF(2).

contends that in Germany, geolocation tools that allow the restriction of access to users from certain countries would probably qualify under the definition of an effective technological measure as 'an access control'.⁷¹¹

The condition of 'effectiveness' most likely reflects the wish of lawmakers to avoid granting protection to obsolete devices or, devices the circumvention of which is too easy. The condition possibly also encapsulates the legislature's intention that the TPM be proportionate to the aim that it pursues. Presumably, a TPM will not be deemed effective if it negatively interferes with the operation of playing or reading equipment. Conversely, it will be deemed effective if it controls the use of protected work through an access or copy-control mechanism (See Article 6(3) InfoSoc Directive). A TPM which prevents access helps reduce illegal reproduction as the mere accessing of a digital work can 'generate' a temporary copy in the user's random access memory (RAM). In addition, access controls underpin the communication and distribution rights.

7.3.10 Limiting access to online content from abroad

Certain TV stations and other online content providers may use geolocation tools to limit access to content. For example, American Netflix accountholders will not be able to download a film if they attempt to access their accounts from outside the US.⁷¹² In addition, sometimes online gaming websites use geolocation tools both to comply with local gaming regulations and to prevent fraud.⁷¹³ Geolocation is used to ensure that customers do not access gaming sites from countries that impose prohibitions or limitations on internet gaming. For example, the online bookmaker William Hill uses geolocation to prevent US players from accessing its gaming products where access would expose the players to liability in their home country.

7.3.11

⁷¹¹ Marketa Trimble, 'The Future of Cybertravel: Legal Implications of the Evasion of Geolocation' (2012) 22 *Fordham Intell Prop Media & Ent LJ* 567, 613, fn 185.

⁷¹² *Ibid* 588, fn 79.

⁷¹³ See generally Julia Hörnle and Brigitte Zammit, *Cross Border Online Gambling Law and Policy* (Edgar Elgar 2010).

7.3.12 *The Accuracy of Geolocation Technology*

As the accuracy of geolocation products is hard to gauge,⁷¹⁴ it is difficult to be categorical about how useful such product will be to private international lawyers. While the manufacturers of the product indicate the potential accuracy to be very high, it has to be borne in mind that they will not be the most unbiased commentators and there may be a tendency to talk the product up.

Some manufacturers of the technology (e.g. Quova) when attempting to parry objections founded on privacy issues, have claimed that accuracy is limited to zip code level and therefore does not pinpoint individual user locations. However, this seemingly modest (and possibly inaccurate) assertion is dismissed by some who claim that Quova is incorporating GPS, Wi-Fi and wireless tower triangulation through Mexens Technology which means that pinpointing of users could be a lot more accurate than mere ZIP code level.⁷¹⁵ It would seem too that a PricewaterhouseCoopers report issued in October 2009 would give the lie to such modesty. That report independently confirmed particularly high levels of country (99.9%) and US State (98.2%) accuracy of Quova's product.⁷¹⁶

Similar levels of accuracy are attributed to server-side geolocation technologies by King in an article written in 2011 and that author observes that that year's accuracy rates reflect substantial increases on those of 2004 when popular geolocation tools were only

⁷¹⁴ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 402.

⁷¹⁵ Chris Silver Smith, 'Geolocation: Core to the Local Space and Key to Click-Fraud Detection' (*Search Engine Land*, 13 August 2007) <<http://searchengineland.com/geolocation-core-to-the-local-space-and-key-to-click-fraud-detection-11922>> accessed 6 July 2012.

⁷¹⁶ Kevin F King, 'Personal Jurisdiction, Internet Commerce, and Privacy: the Pervasive Legal Consequences of Modern Geolocation Technologies' (2011) 21 *Alb LJ Sci & Tech* 61, 70 et seq, fn 21; Marketwire, 'PricewaterhouseCoopers (PwC) Completes Annual Audit of Quova IP Geolocation Data' (14 April 2009) <<http://www.marketwire.com/press-release/pricewaterhousecoopers-pwc-completes-annual-audit-of-quova-ip-geolocation-data-1233911.htm>> accessed 21 August 2012.

80% to 94% accurate at state level. As recently as 2011, server-side technologies could pinpoint a user's location within a twenty to thirty mile radius.⁷¹⁷

Besides the strong endorsement of the technology by PricewaterhouseCoopers, it seems that the technology has achieved sufficient levels of accuracy to be used for legal

⁷¹⁷ Kevin F King, 'Personal Jurisdiction, Internet Commerce, and Privacy: the Pervasive Legal Consequences of Modern Geolocation Technologies' (2011) 21 Alb LJ Sci & Tech 61, 68; Marketwire, 'Quova's Geolocation Data Helps Continental Airlines Improve Web Banner Click-Through Rate by 200 Percent' (24 March 2009) <<http://www.marketwire.com/press-release/quovas-geolocation-data-helps-continental-improve-web-banner-click-through-nyse-cal-1237066.htm>> accessed 21 August 2012. King does however enter a number of important caveats to these calculations. Firstly, server-side accuracy calculations tend to omit consideration of particularly troublesome addresses, such as those associated with America Online (which masks all its users behind proxy servers). Secondly, those calculations assume the absence of users who are intentionally attempting to circumvent the geolocation system via anonymisation tools such as Tor. Thirdly, many accuracy studies do not make allowances for technologies such as wireless Internet access cards and Virtual Private Networks (VPNs) which may cause a user to appear to be connecting from work when the user is in fact travelling in another city or country. Kevin F King, 'Personal Jurisdiction, Internet Commerce, and Privacy: the Pervasive Legal Consequences of Modern Geolocation Technologies' (2011) 21 Alb LJ Sci & Tech 61, 71.

purposes.⁷¹⁸ This became clear in the *Yahoo!* case⁷¹⁹ and in the lower court in the Australian ruling, *Gutnick v Dow Jones & Co Inc.*⁷²⁰

In *Yahoo!*,⁷²¹ Vinton Cerf, the networking guru⁷²² appointed by the presiding judge to the panel of experts advised the judge that determining an individual user's country of origin was unlikely to be possible more than 90% of the time.⁷²³ Justice Gomez concluded that geolocation technologies were sufficiently effective to allow the defendant to implement them to prevent access-seekers located in France from accessing the Nazi memorabilia in question. The perceived existence of feasible technical solutions was determinative in *Yahoo!*⁷²⁴ In addition, the technology was also touched upon by one of the lower courts - the Supreme Court of Victoria - in *Gutnick v Dow Jones & Co Inc.*⁷²⁵ In *Gutnick*, Hedigan J apparently was of the view that a webserver could distinguish between different users' requests based on their physical

⁷¹⁸ Dan Jerker Svantesson, 'Geo-Location Technologies and other Means of Placing Borders on the "Borderless" Internet' (2004) 23 J Marshall J Computer & Info L 101 et seq; Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 421 et seq.

⁷¹⁹ *International League Against Racism & Anti-Semitism (LICRA), French Union of Jewish Students (UEJF) v Yahoo! Inc, Yahoo France*, Interim Court Order, 20 November 2000, Tribunal de Grande Instance de Paris (Country Court of Paris); Yaman Akdeniz, 'Case Analysis of League Against Racism & Antisemitism (LICRA), French Union of Jewish Students (UEJF), v Yahoo! Inc, (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November, 2000' (2001) 1 Electron Bus Law Rep 110-120; Andreas Manolopoulos, 'Raising "Cyber-Borders": the interaction between law and technology' (2003) 11 IJLIT 40, 44. On the *Yahoo!* ruling generally, see Uta Kohl, 'The rule of law, jurisdiction and the internet' (2004) 12 IJLIT 365 – 376.

⁷²⁰ *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 [19], [41] et seq.

⁷²¹ *Yahoo!, Inc v LICRA*, 169 F Supp 2d 1181 (ND Cal 2001).

⁷²² Nicknamed the 'father of the Internet'. 'Geography and the Net – Putting it in its place' *The Economist* (9 August 2001) 20.

⁷²³ Adopting the pragmatic viewpoint that all borders are slightly porous, the French judge in *Yahoo!* decided that a 90% accuracy rate was good enough. 'Geography and the Net– Putting it in its place' *The Economist* (9 August 2001) 20.

⁷²⁴ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 421.

⁷²⁵ *Gutnick v Dow Jones & Co Inc* [2001] VSC 305.

location. It is unfortunate that Justice Hedigan did not provide any support for his conclusion, or indeed, discuss the controversial issues associated with such practice. Further, the matter was not discussed in the subsequent High Court judgment.⁷²⁶

In enhancing localisation on the internet, geolocation technologies directly and inevitably transform the internet from a border disregarding dimension into a medium that takes account of geographical and legal borders. From the perspective of internet regulation, matters may be enhanced by geolocation technology as it makes it possible and practical to consider location online. By helping to define legal borders online, geolocation assists with the application of PIL rules on the internet.

7.3.13 Accuracy of Geolocation Technologies Impugned

Two factors together affect the accuracy of geolocation technologies. They can be divided into two categories: source problems and circumvention problems.⁷²⁷

- (i) **Source Problems:** These are the problems associated with building up and/or collecting accurate geolocation data. As regards IP addresses, there is no real equivalent to the address registers listing physical addresses, or the phone registers listing phone numbers, at least not currently. Consequently, the ones creating databases of geolocation information must rely on other, less straightforward, methods. Clearly, the accuracy of the material in the geolocation databases depends on, and can never be better than, the accuracy of the collection of that data. Thus, the collection of background material is vital. Common methods of collecting relevant material include, for example, gathering data from registration databases,⁷²⁸ network routing information,

⁷²⁶ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 421 et seq.

⁷²⁷ These two sets of problems are dealt with comprehensively in Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 406 et seq.

⁷²⁸ For example, Réseaux IP Européens Network Coordination Centre (RIPE, 'Welcome to the RIPE Network Coordination Centre' <www.ripe.net> accessed 14 August 2012), American Registry for Internet Numbers (ARIN, 'ARIN at a glance' <www.arin.net/about_us/overview.html> accessed 14 August 2012); Asia Pacific Network Information Centre (APNIC, 'About APNIC' <www.apnic.net/about-APNIC/organization> accessed 14 August); Latin American and Caribbean IP Address Regional Registry

DNS systems, host name translations, ISP information and Web content. As discussed in detail by Edelman, all of these sources may provide inaccurate information.⁷²⁹

- (ii) Circumvention Problems: Geolocation technologies can be circumvented by several methods ranging from the technologically advanced (deep linking to streaming video content without accessing the HTTP server) to those easy enough to be used by virtually anyone (anonymizing techniques). One method is inherent in the system structure itself, i.e. tunnelling methods.⁷³⁰ Arguably, the simplest way to circumvent geolocation technologies is through the use of so-called anonymizers. As the name suggests, anonymizers are applications designed to allow web-users to visit websites anonymously. Anonymizers act as an added layer – a buffer – between the web-surfer and the websites he visits.

Where an anonymizer is used, the IP number of the relevant web-surfer is only transmitted to the provider of the anonymizer. A new IP number is then assigned to the web-surfer by the provider and this new IP number will apply in relation to any websites visited by the web-surfer. A web-surfer may request an IP number which indicates a certain country, if the user wishes to give the impression of being physically based in that particular country.

(LACNIC, 'LACNIC Acerca de LACNIC' <lacnic.net/sp/sobre-lacnic/> accessed 14 August 2012).

⁷²⁹ Benjamin Edelman, 'Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television content to Canadian Internet Users' 4 et seq, 11 <http://cyber.law.harvard.edu/archived_content/people/edelman/pubs/jump-091701.pdf> accessed 29 June 2010.

⁷³⁰ Tunnelling methods involve repackaging entire IP packets so as to send them to their destination via a remote tunnelling server, thereby hiding a user's actual location and causing the user to appear to hold the IP address of her tunnelling server. These methods are widely deployed in the context of corporate networks and the end user's necessary client software is included with recent versions of Microsoft Windows operating system. Ibid 9.

While geolocation technologies may be circumventable, this fact must be seen in the context of general and inevitable regulatory slippage which is a fact of life in both worlds - the online and offline.⁷³¹

7.3.14 The Growing Influence of Geolocation Technology in the Courts

The courts are to an increasing degree taking account of geo-identification.⁷³² In some fairly recent cases, the courts have recognised the value of existing geolocation technologies. For example, in *National Federation of the Blind v Target Corporation*, the court stated the following:

Pataki asserts that someone who puts content on the internet has ‘no way to determine the characteristics of their audience...[such as] age and geographical location.’ Pataki, 969 F. Supp. at 167. This is simply incorrect. It is common practice for websites, for entities operating in multiple countries to have a single site that directs customers to different versions based upon language. Websites can determine the location of a user from information they provide, such as a credit card number, or from the internet service provider that an individual uses. It may or may not be prohibitively expensive for a website to tailor its content based on the location of its users, but it is certainly technically feasible.⁷³³

⁷³¹ Ibid 4 et seq, 9. Goldsmith and Sykes argue that the presence of imperfections in a particular technology is not necessarily synonymous with infeasibility/ineffectiveness. They point out that regulation works by raising the cost of the proscribed activity, and not necessarily by eliminating it. While computer savvy users might always be able to circumvent identification technology, they do so at a certain cost and that cost is prohibitive for most. Jack L Goldsmith and Alan O Sykes, ‘The Internet and the Dormant Commerce Clause’ (2001) 110 Yale LJ 785, 812.

⁷³² Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 422; Kevin F King, ‘Personal Jurisdiction, Internet Commerce, and Privacy: the Pervasive Legal Consequences of Modern Geolocation Technologies’ (2011) 21 Alb LJ Sci & Tech 61, 71.

⁷³³ *National Federation of the Blind v Target Corp*, 452 F Supp 2d 946, 961 et seq (ND Cal 2006)

In the 2007 ruling, *Hageseth v Superior Court*,⁷³⁴ the court took note of the emergence of geolocation technologies and demonstrated that it was clearly eager to encourage the development of technologies which it saw as helpful to law enforcement. The case concerned the alleged illegal prescription (over the internet) of medicine by an out-of-state medical practitioner. The dispute related to whether a Californian court could exercise jurisdiction over the Colorado-based doctor.⁷³⁵ The court stated as follows:

The prospect of other technological developments counsels judicial caution in accepting technology-based arguments against the assertion of jurisdiction, as that would eliminate incentives for technology developers to innovate in ways that would facilitate law enforcement and support public values.⁷³⁶

Two German internet gambling cases from 2008 involve discussion of geolocation technologies. In the VGH Bayern, 10 CS 08.2399 ruling,⁷³⁷ handed down by the Bavarian Administrative Court, banner advertising for private sports bookmakers was at issue. The court held that the enforcement authorities of a federal state ('land') could order a cessation of banner advertising for lawful, private sports bookmakers but that the order had to be limited to the territory of the particular federal state (Bavaria). The court accepted an expert report by Professor Thomas Hoeren that geolocation tools were effective on a nationwide basis for about 99 per cent of cases. In effect, the court upheld the enforcement order on the basis that providers could use geolocation tools to restrict the effects of the prohibition and manage their compliance risks (so that the advertisement could still be seen, for example in other countries, where such advertisements might be legal).⁷³⁸ The vacillating fortunes of geolocation tools is demonstrated by the OVG Thüringen decision⁷³⁹ in which the Higher Administrative Court in Thuringia found that the internet gambling prohibition could not be enforced

⁷³⁴ *Hageseth v Superior Court of San Mateo County*, 150 Cal App 4th 1399; 59 Cal Rptr 3d 385; Cal Daily Op Service 5647 (2007).

⁷³⁵ Account of this case taken from Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 423.

⁷³⁶ *Hageseth v Superior Court of San Mateo County*, 150 Cal App 4th 1399; 59 Cal Rptr 3d 385; Cal Daily Op Service 5647 (2007) [54].

⁷³⁷ Handed down 20th November 2008.

⁷³⁸ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 424 et seq.

⁷³⁹ OVG Thüringen 03.12.2008, 3 EO 565/07.

against an out-of-state provider, as geolocation tools were deemed not sufficiently precise.⁷⁴⁰

It is not just the courts which have taken account of geolocation technologies. Certain statutes have been drafted in a way which suggests that the legislator expects website operators to apply some form of geo-identification. Examples frequently arise in the context of regulation of online gambling. A good example is Section 6(1) of the Australian Interactive Gambling Act 2001, which reads as follows:

‘For the purposes of this Act, a prohibited Internet gambling service is a gambling service, where: (...) (c) an individual who is physically present in Australia is capable of becoming a customer of the service.’

The Explanatory Memorandum to the Act shows that the drafters were aware of geolocation technologies.⁷⁴¹

As to the future of geolocation technology, it has been argued that the new version Internet Protocol - IPv6 – would enhance the accuracy of geolocation technologies. In fact, it has been said that IPv6 would make the identification of the physical location of an internet user a rather trivial task.⁷⁴² Jacobus contends that by expanding the IP address system, IPv6 would make people more easily identifiable by assigning serial numbers to each computer’s network-connection hardware.⁷⁴³

⁷⁴⁰ Svantesson also makes the point that any assessment of the value of geo-identification must be context-specific. Thus, courts may well conclude that geolocation technologies are sufficiently accurate in one context, but not in another context. Svantesson believes that it would be an error for a court to dismiss geolocation technologies as insufficiently accurate where such a dismissal is guided only by another court having reached such a conclusion before it - Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 425.

⁷⁴¹ The Parliament of the Commonwealth of Australia, ‘Interactive Gambling Bill 2001 Revised Explanatory Memorandum’ (1998-1999-2000-2001) 54
<http://www.archive.dcita.gov.au/__data/assets/pdf_file/0016/11536/Interactive_Gambling_Bill_2001_Revised_Explanatory_Memorandum.pdf> accessed 14 August 2012.

⁷⁴² Stefanie Olsen, ‘Geographic tracking raises opportunities, fears’ (*CNET News*, 8 November 2000) <<http://news.cnet.com/2100-1023-248274.html>> accessed 6 July 2012.

⁷⁴³ Patricia Jacobus, ‘Building fences, one by one’ (*CNET News*, 19 April 2001) <<http://news.cnet.com/2009-1023-255774-2.html>> accessed 6 July 2012.

While the ultimate plan may be to replace IPv4 with IPv6, the transition is progressing very slowly and IPv4 is still the dominant version in use.⁷⁴⁴ 2014 statistics prepared by Google indicate that IPv6 penetration is somewhere between 3% and 4%, and this despite the fact that the version is now 16 years old.⁷⁴⁵ It is widely expected that IPv4 will be supported alongside IPv6 for the foreseeable future. (IPv4-only nodes are not able to communicate directly with IPv6 nodes, and will need assistance from an intermediary.)

Importantly, there is not absolute consensus that IPv6 will actually improve the accuracy of geolocation technologies. Diminished accuracy may arise from the fact that IPv6 will allow ISPs to dynamically reassign their address ranges at any time.⁷⁴⁶ With no actual geographic constraint under IPv6, these IP address blocks could be reassigned to a new area at any time that demand shifts. As the internet continues to expand and the need for renumbering grows, blocks of IP addresses will be shifted geographically with increasing regularity. Keeping track of all the growing number of reassignments of IP addresses may overwhelm geolocation software's capabilities. In addition, during the multi-year global transition to IPv6, dual sets of router table data will have to be maintained for both IPv4 and IPv6 addresses. The need to translate and correlate between tables may also introduce latency that negatively impacts the ability to conduct real time analysis.⁷⁴⁷

⁷⁴⁴ Penn Computing, 'IPv6 (Internet Protocol version 6) at Penn' (*University of Pennsylvania*) <<http://www.upenn.edu/computing/ipv6/>> accessed 14 August 2012.

⁷⁴⁵ Google, 'IPv6 Statistics' (1 June 2014) <<https://www.google.com/intl/en/ipv6/statistics/html>> accessed 3 June 2014.

⁷⁴⁶ One view is that the vast amount of address space available under IPv6 will likely eliminate the need for ISPs to assign dynamic IP addresses. The shift from dynamic to static will in turn make it easier to focus on the individual user via IP-based geolocation. Kevin F King, 'Personal Jurisdiction, Internet Commerce, and Privacy: the Pervasive Legal Consequences of Modern Geolocation Technologies' (2011) 21 Alb LJ Sci & Tech 61, 120.

⁷⁴⁷ Tinabeth Burton, 'US industry group white paper says geolocation technologies are not precise enough to identify taxing jurisdiction reliably, rendering EU VAT rules unworkable' (*THE*, 29 October 2002) <<http://www.timeshighereducation.co.uk/story.asp?storyCode=172460§ioncode=26>> accessed 30 June 2010 which refers to Information Technology Association of America (ITAA), 'ECommerce Taxation and the Limitations of Geolocation Tools' 7 <<http://www.sethf.com/nitke/geolocationpaper.pdf>> accessed 14 August 2012.

Edelman agrees with the contention that geolocation technology's accuracy is likely to decrease in the future.⁷⁴⁸ It should be borne in mind however that his discussion paper referred to retransmission of over-the-air television on the internet and was written on behalf of the National Association of Broadcasters (Canada). The reasons he relies on are, however, persuasive and include a perceived rise in the deployment of proxy servers, tunnelling systems and terminal services, an increase in the deployment of mobile network devices and a likely increase in the availability of automated tools or generally known methods for circumventing geolocation technologies.

There is a risk too that the improvements in and development of geolocation technology may be sub-optimal. This arises from the fact that Digital Envoy, a geolocation service provider, was granted a patent⁷⁴⁹ in mid-2004 which Digital Envoy claims covers the core methods used by geolocation technologies focused on IP numbers. Digital Envoy stated that it plans to defend its patent aggressively⁷⁵⁰ and one of the company's co-founders said that it was unlikely that any other provider would be able to offer accurate geolocation solutions without infringing Digital Envoy's patent. Such utterances imply one dominant player in the sector which may not bode well for a fast evolution of the technology.

7.3.15 Possible Legal Obstacles to the use of Geolocation Technology

Besides the accuracy issue, another potential obstacle to the widespread use of geolocation technologies is if IP addresses were considered 'personal data' or 'personal

⁷⁴⁸ Benjamin Edelman, 'Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television content to Canadian Internet Users' 11 <http://cyber.law.harvard.edu/archived_content/people/edelman/pubs/jump-091701.pdf> accessed 29 June 2010.

⁷⁴⁹ United States Patent 6,757,740 titled 'Systems and Methods for Determining, Collecting and Using Geographic Locations of Internet Users'.

⁷⁵⁰ Stefanie Olsen, 'Digital Envoy wins geotargeting patent' (*CNET News*, 29 June 2004) <http://www.news.cnet.com/Digital-Envoy-wins-geotargeting-patent/2110-1032_3-5251844> accessed 30 June 2010.

information' for privacy purposes. If so, their collection, use and disclosure could be seriously restricted.⁷⁵¹

In its Opinion 4/2007, the Article 29 Data Protection Working Party confirmed that they consider IP addresses as constituting data relating to an identifiable person.⁷⁵² Referring to the example of dynamic IP addresses in their Opinion, the Working Party use the example of internet access providers and managers of local area networks who, 'using reasonable means', are able to identify internet users to whom they have attributed IP addresses as they normally systematically 'log' in a file the date, time, duration and dynamic IP address given to the internet user. The same argument can be made in relation to ISPs who keep logbook on the HTTP server. The Article 29 Working Party considers the IP addresses provided by internet access providers and ISPs to constitute personal data within the meaning of Article 2(a), Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.⁷⁵³

⁷⁵¹ Perhaps naturally, the developers of geolocation technologies argue that their products are 'non-invasive' and 'privacy safe'. As regards the 'non-invasive' assertion, see Digital Envoy, 'Digital Envoy Alliance with Melbourne IT gives global boost to innovative internet marketing and eCommerce technology; hoping to avoid "Cookies" controversy, Australian firm embraces NetAcuity as the emerging standard for non-invasive web tracking and customer service activities' (9 April 2000) <http://www.digitalenvoy.net/news/press_releases/2000/pr_040900.html> accessed 14 August 2012; as regards the 'privacy safe' assertion, see Quova, 'Technical Overview of GeoPoint' <http://www.quova.com/technology/quova_tech_whitepaper.pdf> accessed 30 June 2010.

⁷⁵² Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (1248/07/EN, WP 136, 20 June 2007) 16 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> accessed 6 July 2012.

⁷⁵³ For two Paris Appeals Court rulings (2007) holding that IP addresses do not facilitate the identification of persons who used the computer since only LEAs may obtain user identity from the ISP, see a summary of *Anthony G v SCPP* in French: Legalis, 'Cour d'appel de Paris, 13ème chambre, section B, Arrêt du 27 avril 2007' (LEGALISnet, 27 April 2007) <http://www.legalis.net/jurisprudence-decision.php3?id_article=1954> accessed 6 July 2012; and see a summary of *Henri S v SCPP* in French: Legalis, 'Cour d'appel de Paris 13ème chambre, section A, Arrêt du 15 mai 2007' (LEGALISnet, 15 May 2007) <http://www.legalis.net/jurisprudence-decision.php3?id_article=1955> accessed 6 July 2012.

In the Information Commissioner's Office's (ICO) Good Practice Note titled 'Collecting Personal Information Using Websites',⁷⁵⁴ a distinction is drawn between dynamic IP addresses and static IP addresses. In the ICO's opinion, dynamic addresses *without* any other identifying or distinguishing information cannot be covered by the UK's Data Protection Act 1998 since only ISPs can link the IP address to an individual. In contrast, the ICO deems a static address and its related profile (the linking of an IP address to a particular computer which is, in turn, linked to an individual user) to constitute personal information and are therefore covered by the provisions of the 1998 Act.

In January 2008,⁷⁵⁵ Germany's data protection commissioner, Peter Scharr, told a European Parliament hearing on online data protection that when someone is identified by an IP address, then it should be regarded as personal data. Mr Scharr was speaking in his capacity as leader of the EU group tasked with the job of preparing a report on how well the privacy policies of internet search engines operated by Google, Yahoo, Microsoft and others comply with EU privacy law.⁷⁵⁶

As regards the situation in the US, in *State of New Jersey v Reid*,⁷⁵⁷ the New Jersey Supreme Court ruled (in April 2008) that an IP address could constitute 'personally identifiable information' (PII) (the US equivalent term for personal data) and consequently ISPs were not entitled to disclose such addresses to the police without a

⁷⁵⁴ Information Commissioner's Office (ICO), 'Good Practice Note - Collecting personal information using websites' (3 June 2007) 3

<http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf> accessed 30 June 2010.

⁷⁵⁵ Aoife White, 'IP Addresses Are Personal Data, E.U. Regulator Says' (The Washington Post, 22 January 2008) <<http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html>> accessed 30 June 2010.

⁷⁵⁶ For a recent Irish High Court ruling (16 April 2010) holding that an IP address does not constitute personal data under Ireland's Data Protection Acts, 1988-2003, see *EMI Records & Ors v Eircom Ltd* [2010] IEHC 108 [25] (Charleton J).

⁷⁵⁷ *State of New Jersey v Shirley Reid*, 194 NJ 386, 954 A2d 503 (NJ 2008) (Rabner CJ), writing for a unanimous Court.

grand jury subpoena.⁷⁵⁸ Interestingly, the New Jersey court's analysis went beyond IP addresses and seemed to indicate that clickstream data associated with particular addresses might attract privacy protection as well. However, the situation became somewhat confused in 2009 when the US District Court for the Western District of Washington⁷⁵⁹ held that IP addresses do not constitute PII. The ruling, *Johnson v Microsoft Corp*, involved a claim that Microsoft had collected consumer IP addresses during the Windows XP installation process, an action that the plaintiffs argued violated the XP End User License Agreement.⁷⁶⁰ In granting summary judgment in favour of Microsoft, US District Court Judge Richard A Jones found that 'In order for "personally identifiable information" to be personally identifiable, it must identify a person. But an IP address identifies a computer'.⁷⁶¹

As for US legislation, it is arguable that a clearer picture emerges when one analyses the term 'personal information' contained in the Children's Online Privacy Protection Act of 1998 (COPPA). Under Section 1302(8) of that statute, the term 'personal information' means 'individually identifiable information about an individual collected online', to include such things as first and last name, a home or other physical address including street name and name of a city or town, an email address, a telephone number and 'any other identifier that the Commission⁷⁶² determines permits the physical or online contacting of a specific individual' (category (F)). It is almost certain that IP addresses would fall under (this) category (F) of Section 1302(8).⁷⁶³

⁷⁵⁸ Wendy Davis, 'Court Rules Web Users Have Expectation of Privacy' (*MediaPost*, 24 April 2008) <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=81306> accessed 1 July 2010.

⁷⁵⁹ at Seattle.

⁷⁶⁰ The XP End User License Agreement stated that Microsoft would not collect PII without the user's consent. The Plaintiffs referenced Microsoft's own online glossary to support their claim that IP addresses should be considered PII. The glossary defined 'personally identifiable information' as 'any information relating to an identified or identifiable individual. Such information may include (...) IP address.'

⁷⁶¹ *Johnson v Microsoft Corp*, C06-0900RAJ-WD Wa 06/23/09, 2009 WL 17934400, III B 3.

⁷⁶² Federal Trade Commission.

⁷⁶³ This point is made by the Electronic Privacy Information Centre under the heading 'Key Definitions' / 'Personal Information'. EPIC, 'Children's Online Privacy Protection Act (COPPA)' <<http://epic.org/privacy/kids/>> accessed 3 July 2010.

What implications flow from a situation where IP addresses are deemed by the courts to constitute personal data/PII? In brief, companies that use IP addresses for business purposes (e.g, manufacturers of geolocation technology) would be required to comply with data protection laws. Additionally, the internet users to which the IP addresses relate would have important data subject rights under general data protection legislation. For example, in the UK, the internet users could rely on data protection principles 1 and 6 (contained in Schedule 1, Part 1) of the DPA 1998.⁷⁶⁴ They provide as follows: that personal data be processed fairly and lawfully ('processing' includes disclosure of the data by transmission, dissemination or otherwise making available)⁷⁶⁵ (Principle 1), and that the personal data be processed in accordance with the rights of the data subject under the Act (Principle 6).

7.3.16 Some Conclusions on Geolocation Technology

Weighing up the benefits and disbenefits of geolocation technology and then coming up with an overall verdict is not an easy task. It seems clear enough that the technology has attained high levels of accuracy but sometimes even the accuracy rates can justifiably be impugned as in the instance of PricewaterhouseCooper's audit of its own client's technology. Such a scenario does not really engender thoughts of independent, objective assessment.

The other worrying issue about accuracy levels is that doubt has been expressed about whether IPv6 would actually enhance accuracy levels within geolocation technologies. But, worryingly, even if IPv6 would enhance accuracy, this new protocol is being rolled out at glacial speeds.

On the plus side, the technology seems to have established an important foothold in legal proceedings as demonstrated in the *Yahoo!* and *Gutnick* cases. Svantesson correctly observes that the courts acknowledgement and use of the technology will create a strong incentive for its development. In time, this should create a virtuous circle

⁷⁶⁴ For a comprehensive treatment of the data protection principles, see Ian Lloyd, *Cyber Law in the United Kingdom* (Kluwer Law International 2010) 181 et seq; Ian J Lloyd, *Information Technology Law* (6th edn, OUP 2011) ch 5.

⁷⁶⁵ Children's Online Privacy Protection Act of 1998, Sections 1302(4), 1303(a)(1).

whereby likely improved accuracy levels will influence the courts to attach even greater importance to the technology.

In his work, *Private International Law and the Internet* Svantesson states that

geolocation technologies should not be seen as an alternative to using private international law to erect protective borders on the internet. Rather, the application of private international law must recognise the value of both geolocation technologies and non-technical geo-identification for the identification of geographical location.⁷⁶⁶

This, in fact, is a very pragmatic approach to a situation which should lead naturally to a symbiotic relationship between the law (PIL) and technology (geolocation technology). It would seem that there is a golden opportunity for conflicts lawyers to embrace a technology that may assist them greatly to establish physical borders in the online world. Given the serious and undeniable challenges of applying PIL rules to the internet, private international lawyers need all the assistance they can get. It may well be that geolocation technology improves to such an extent that the IP addresses of infringing computers, tablets, i-Pads etc can be traced, thereby giving copyright holders/private international lawyers a distinct advantage in terms of trying to localise the *locus delicti*.

One potential weakness with geolocation technology is the strengthening viewpoint that IP addresses constitute personal data/PII. While there have been court rulings in the US, France and Ireland upholding the counter-argument, the consensus now seems to point towards IP addresses constituting personal data.

This includes an Article 29 Working Party Opinion.⁷⁶⁷ Serious implications flow from the consensus. If the collectors/providers of the geolocation data hold IP addresses, then they will be subject to onerous data controller duties (also involving costly data protection outlays).

⁷⁶⁶ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 441.

⁷⁶⁷ Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (1248/07/EN, WP 136, 20 June 2007) 16 <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> accessed 6 July 2012.

7.4 The Third Facilitative Element – Data Retention Legislation

The aim of this part of the chapter is to set out data retention legislation that may assist (or facilitate) a prejudiced copyright owner in terms of suing an IP infringer. In my analysis, I shall focus on the specific provisions that potentially assist the copyright owner the most. Any potential assistance to the copyright owner will be evidential in nature and most likely corroborative in nature. Such evidence will take the form of data (internet/mobile phone) retained by ISPs and Telcos under their data retention obligations, originally prescribed by Directive 2006/24/EC, a legal instrument recently held to be invalid by the CJEU in *Joined cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications; and Kärntner Landesregierung*.⁷⁶⁸

However, for the hypothetical assistance (retained data) to evolve into tangible assistance (evidence to be adduced in a civil case), a court order such as a *Norwich Pharmacal* Order would ultimately be needed by the rightholder to oblige the ISP to disclose the relevant data. In turn, this data (name and address of a subscriber to an ISP service, for example) could be used to institute court proceedings against that subscriber who is suspected of copyright infringement.

Despite the momentous ruling by the EU's most senior court in April, it is important to bear in mind that the UK's transposing regulations are still valid (though the option remains for national courts and administrations to dis-apply these national provisions if they wish). While there is no automatic effect on national legislation following the Luxembourg decision, Member States seem to have the alternative between:

- Abrogating the entire national data retention legislation; or
- Modifying the national data retention legislation so as to meet the proportionality concern of the CJEU

Given the finding of invalidity against the Directive, there does not seem to be much point in analysing it. Instead, what I propose doing is to analyse the most important provisions of the UK transposing legislation and then to take a look at the CJEU's recent ruling and its general implications for data retention in the EU.

⁷⁶⁸ *Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; and Kärntner Landesregierung* (CJEU (Grand Chamber) 8 April 2014).

As the UK data retention obligations are inspired (and required!) by EU legislation, it is my intention to first treat Directive 2006/24/EC and then examine how this Directive has been transposed into UK legislation.

I shall then critically evaluate the relevant provisions of the UK legislation, the objective being to assess how potentially useful they are from a prejudiced rightholder's perspective. This all links back to the key task of determining the identity of the online infringer, so as to allow Article 2, Brussels I, to apply.

It is acknowledged that the usefulness of the data retention obligations (from the perspective of a prejudiced rightholder) is somewhat fortuitous/serendipitous, given that the rationale behind the now invalidated Directive 2006/24/EC was to ensure that data be available for the investigation, detection and prosecution of serious crime.⁷⁶⁹ But, frequently, legislation adopted to achieve a particular purpose can have happy unintended consequences for individuals or sectors of society not originally envisaged by the drafters of said legislation.

7.4.1 How Directive 2006/24/EC was implemented into UK law

The Data Retention Directive was transposed into UK law by way of secondary legislation. The first set of Regulations (SI 2007/2199) was adopted in July 2007 and came into force on 1st October 2007. However, these excluded retention of records from internet communications. After a somewhat tortuous process, the 2007 Regulations were eventually superseded by Data Retention (EC Directive) Regulations 2009 (SI 2009/859) from April 2009.⁷⁷⁰

⁷⁶⁹ See the view of Bob Stankey, 'UK ISPs to begin storing Internet traffic data' (ACC, 19 February 2009) <<http://www.lexology.com/library/detail.aspx?g=0abfe79d-00a2-4532-8dea-5e6281efef64>> accessed 16 April 2014. He states that whilst the original rationale for communications data retentions was to help prevent terrorism, investigate murders and prosecute other serious crimes, they will also allow the authorities to use the information to crack down on online piracy and copyright infringements. He goes on to state: 'this means that ISPs can be asked for IP addresses and subscriber names and addresses in order to take action against illegal file-sharers'.

⁷⁷⁰ Interestingly, in its draft Legislative Programme, (Cm 7372, 2008) the UK government included a proposal for a Communications Data Bill. The proposal was linked to the government's Intercept Modernisation Programme and the Bill would have provided for the

7.4.2 Data Retention (EC Directive) Regulations 2009

The 2009 Regulations complete the transposition of Directive 2006/24/EC into domestic law in the UK. They came into force on 6 April 2009. In effect, the 2009 regulations make the retention of communication data mandatory rather than voluntary. There are two key provisions within the 2009 Regulations. They are Regulation 4 which obliges public communications providers to retain communications data specified in the Schedule to the Regulations and Regulation 5 which specifies the retention period with which public communications providers must comply. They are obliged to retain the data for a period of 12 months from the date of the communication in question.

Under the 2009 Regulations, the type of data that must be retained includes data generated or processed by means of mobile telephony, internet access, internet e-mail and internet telephone. Given that the four means of communication just mentioned are all conducive to digital copyright infringement, data generated therefrom could potentially constitute strong, albeit indirect evidence of digital copyright infringements.

7.4.3 The communications data to be retained under the Schedule to the Regulations

Part 3 of the Schedule relates to internet access, internet e-mail or internet telephony. In terms of data necessary to trace and identify the source of a communication, the following data must be retained under paragraph 11 of Part 3:

- The user ID allocated
- The user ID and telephone number allocated to the communication entering the public telephone network

collection and retention of further communications data not required by the Directive. Controversy ensued however when it was reported that the creation of a central database of all electronic communications was to be part of the programme. The government dropped the proposed Bill in the face of rising opposition. See Alex Hunt, 'David Cameron wants fresh push on communications data' (*BBC News Politics*, 30 January 2014) <<http://www.bbc.co.uk/news/uk-politics-25969918>> accessed 3 June 2014.

- The name and address of the subscriber or registered user to whom an IP address, user ID or telephone number was allocated at the time of the communication

Data necessary to identify the destination of a communication is covered by paragraph 12 of Part 3. As regards internet telephony, the user ID or telephone number of the intended recipient of the call must be retained. In the case of e-mail, the name and address of the subscriber or registered user and the user ID of the intended recipient of the communication must be retained.

Paragraph 13 of Part 3 pertains to data necessary to identify the date, time and duration of a communication.⁷⁷¹ The provision divides the data into 2 categories, firstly data relating to internet access and secondly, data relating to e-mail or internet telephony:

As regards the former, the following (data) must be retained:

- The date and time of the log-in and the log-off from the internet access service, based on a specified time zone
- The IP address, whether dynamic or static, allocated by the internet access service provider to the communication, and
- The user ID of the subscriber or registered user of the internet access service

As regards e-mail or internet telephony, the data to be retained includes the date and time of the log-in to and log-off from the e-mail or internet telephony service, based on a specified time zone.

Data necessary to identify the type of communication is governed by paragraph 14 of Part 3. It provides that in the case of internet e-mail or internet telephony, data relating to the internet service used, must be retained.

Data necessary to identify users' communication equipment must also be retained. Paragraph 15 states that in the case of dial-up access, the calling telephone number must be retained while in all other cases, the digital subscriber line (DSL) or other end point of the originator of the communication must be retained.

⁷⁷¹ These requirements are set out in provision 13 of Part 3 of the Schedule.

Importantly, the phenomenon of ‘scope creep’ may affect the 2009 regulations, whereby data retained for one purpose – law enforcement – can also be used for other purposes. Lobbying by industry which might instigate such scope creep has already occurred in the UK. There, the Creative and Business Media Association (CMBA) representing the digital content industry demanded that access to retained data should also be granted for the purpose of investigating other crimes, such as IP infringement. This could lead to a situation where an instrument brought in as an anti-terrorist measure may, in the future, be used to prosecute illegal file-sharers.⁷⁷²

7.4.4 CJEU’s ruling in Digital Rights Ireland

*Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and others.*⁷⁷³

This landmark ruling represents a privacy victory that makes subsequent drafting of data retention rules in a copyright environment problematical insofar as concern for fundamental rights may not have been adequately factored into earlier case law in England and Wales in particular.

In drafting a replacement Data Retention Directive, the European Commission will have to acknowledge the strength of the fundamental rights enshrined in Articles 7 and 8 of the Charter and ensure that they are not disproportionately interfered with.

7.4.5 A Preliminary Ruling concerning the validity of Directive 2006/24/EC

This request for a preliminary ruling concerned the validity of Directive 2006/24/EC on the retention of data generated or processed in connection with the provision of publicly

⁷⁷² Judith Rauhofer, ‘The Retention of Communications Data in Europe and the UK’ Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009) 596.

⁷⁷³ Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; and Kärntner Landesregierung* (CJEU (Grand Chamber) 8 April 2014).

available electronic communications services or of public communications networks. One of the requests was made by the Irish High Court while the other was made by the Austrian Verfassungsgerichtshof (Constitutional Court).

In essence, the referring courts were asking the CJEU to examine the validity of Directive 2006/24 in the light of Articles 7,⁷⁷⁴ 8,⁷⁷⁵ and 11⁷⁷⁶ of the Charter of Fundamental Rights of the European Union.⁷⁷⁷

The CJEU examined the question of whether the interference caused by Directive 2006/24 is limited to what is strictly necessary. It was observed that by virtue of its Articles 3 and 5(1), the directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, internet access, internet e-mail and internet telephony. It therefore applies to all means of electronic communication, the use of which is very widespread and of growing importance. Furthermore, by virtue of Article 3, the directive covers all subscribers and registered users. It therefore entails an interference with the fundamental rights of practically the entire European population.⁷⁷⁸

The court was critical of the directive's overbroad application which affects persons using electronic communication services even if there is little prospect of criminal prosecutions occurring. The directive's lack of exceptions also meant that it would apply to persons whose communications were subject to the obligation of professional secrecy.⁷⁷⁹

⁷⁷⁴ Article 7 refers to respect for private and family life. It states that 'everyone has the right to respect for his private and family life, home and communications'.

⁷⁷⁵ Article 8 refers to the protection of personal data. It provides that everyone's personal data should be protected and that data must only be processed fairly for specified purposes and on a consensual basis. It also specifies that compliance with the data protection rules be subject to control by an independent authority.

⁷⁷⁶ Article 11 enshrines the right to freedom of expression and information.

⁷⁷⁷ Charter of Fundamental Rights of the European Union [2000] OJ C364/01.

⁷⁷⁸ Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; and Kärntner Landesregierung* (CJEU (Grand Chamber) 8 April 2014), para 56.

⁷⁷⁹ *Ibid* 58.

7.4.6 The General absence of limits

Secondly, the CJEU referred to the ‘general absence of limits’ in the directive and its failure to lay down any objective criterion by which to determine the limits of access by the competent national authorities to the data and their subsequent use.⁷⁸⁰ Article 4 of the directive, which governs the access of the national authorities to the data retained does not expressly provide that that access and the subsequent use of the data in question must be strictly restricted to the purpose of preventing and detecting serious offences or of conducting criminal proceedings relating thereto.⁷⁸¹

Problematical too was the fact that access by the competent national authorities to the data retained was not made dependent on a prior review carried out by a court or by an independent administrative body, whose decision would seek to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued.⁷⁸²

7.4.7 The data retention period

Thirdly, as regards the data retention period of between 6 months and 24 months, no distinction is made between the categories of data set out in Article 5 of the directive on the basis of their possible usefulness. Nor is the determination of the period of retention based on objective criteria in order to ensure that it is limited to what is strictly necessary.⁷⁸³

7.4.8 Interference with the fundamental rights set out in the Charter

In what is probably the most compelling passage of the ruling, the CJEU, at paragraph [65], criticised the Directive for not laying down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter. The court then went on to hold that Directive 2006/24 involves a wide-

⁷⁸⁰ Ibid 61.

⁷⁸¹ Ibid.

⁷⁸² Ibid 62.

⁷⁸³ Ibid 64.

ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary.⁷⁸⁴

7.4.9 The rules relating to security and protection

The CJEU was also critical of the rules relating to security and protection of data retained by providers of publicly available electronic communications services. It ruled that Directive 2006/24 does not provide for sufficient safeguards as required by Article 8 of the Charter, to ensure effective protection of the retained data against the risk of abuse and against any unlawful access and use of that data.⁷⁸⁵ Elaborating on this, the court held that Article 7 of Directive 2006/24, the provision governing data protection and data security, does not lay down rules which are specific and adapted to (i) the vast quantity of data whose retention is required by that directive, (ii) the sensitive nature of the data and (iii) the risk of unlawful access to that data. Such rules, if implemented, would serve to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality.

Assessing Article 7 of Directive 2006/24 in conjunction with the Article 4(1) of Directive 2002/58 and Article 17(1) of Directive 95/46, the court stated that cumulatively, the three provisions did not ensure a ‘particularly high level of protection and security’.⁷⁸⁶ The CJEU was also particularly critical of the fact that Directive 2006/24 does not ensure the irreversible destruction of the data at the end of the data retention period.⁷⁸⁷

Staying with the issue of security and protection of data, the court noted that the directive does not require the data in question to be retained within the European Union. As a consequence, the directive failed to comply with Article 8(3) of the Charter which requires that compliance with the protection of personal data rules be ‘subject to control

⁷⁸⁴ Ibid 65.

⁷⁸⁵ Ibid 66.

⁷⁸⁶ Ibid 67.

⁷⁸⁷ Ibid.

by an independent authority'.⁷⁸⁸ This reference to an independent authority is to the national data protection authority operating in each of the 28 Member States. If the data were retained outside the borders of the EU, then the power, control and influence of the EU data protection authorities would be negligible. As stated in *Commission v Austria* previously, such control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data.⁷⁸⁹

7.4.10 Outcome of the case

Having regard to all the foregoing considerations, the CJEU ruled that by adopting Directive 2006/24, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1)⁷⁹⁰ of the Charter.⁷⁹¹ As a consequence, the court found Directive 2006/24 to be invalid.

7.4.11 Implications of the ruling

The *Digital Rights Ireland* judgment is undoubtedly a landmark ruling. It is only the second time ever that the CJEU has struck down an EU directive⁷⁹² and the ruling comes at an important time when there is an ongoing debate in both the EU and US, sparked by Edward Snowden's revelations of the spying activities of the US National Security Agency. Tangibly, the ruling will serve to limit blanket government surveillance of communications data, which was permitted under the directive.

⁷⁸⁸ Ibid 68.

⁷⁸⁹ Case C-614/10 *European Commission v Austria* [2013] 1 CMLR 23, para 34.

⁷⁹⁰ Article 52(1) of the Charter refers to the scope and interpretation of rights and principles. It provides that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. All limitations are subject to the principle of proportionality and may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

⁷⁹¹ Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; and Kärntner Landesregierung* (CJEU (Grand Chamber) 8 April 2014), para 69.

⁷⁹² On the other occasion, the ECJ held that the legislation prohibiting tobacco advertising had been established on improper grounds.

A period of legal uncertainty is inevitable particularly as the court held that the declaration of invalidity would take effect from the date on which the directive entered into force. This element of retrospection could seriously impact the outcome of proceedings long since concluded where the evidence relied on was data retained under the directive. There is also a strong likelihood that national legislation transposing the directive will now be challenged in domestic courts.

As the Directive is entirely invalid, the immediate consequence is that we return to the status quo before 2005. This means that Member States have an option, not an obligation to retain data pursuant to the e-Privacy Directive.

It is difficult to see domestic legislation avoiding censure if it reflects the elements of the Directive which have already been found wanting by the EU's most senior court. The prospect of the EU legislature adopting a replacement directive in early course is unlikely. However, if there is to be a new Directive, it may be included in the main data protection package being negotiated by the EU institutions.⁷⁹³

While there is no obvious silver bullet for this imbroglio, the ruling may well help to steel the resolve of those in Europe who have been clamouring for a Digital Bill of Rights which would enshrine the right of privacy for digital citizens using the internet.

Somewhat ironically, such data was already being retained by some service providers under the voluntary Code of Practice on the Retention of Communications Data (2003), a code which had been established under the 2001 Anti-Terrorism, Crime and Security Act (ATCSA). I shall now examine the Anti-Terrorism, Crime and Security Act 2001

⁷⁹³ This comprehensive reform of the EU's data protection rules was announced by the European Commission on 25th January 2012 so as to strengthen online privacy rights and boost Europe's digital economy. Two legislative proposals are included in the reforms – a Regulation setting out a general EU framework for data protection and a Directive on protecting personal data processed for the purposes of prevention, detection, investigation or prosecution of criminal offences and related judicial activities. See European Commission press release titled 'Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their data and to cut costs for businesses' (IP/12/46, 25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm> accessed 16 April 2014.

7.4.12 The Anti-Terrorism, Crime and Security Act 2001

Separately, there has existed for quite some time in the UK, a distinct piece of legislation which provides a legal basis for the retention of communications data for certain purposes, namely, the Anti-Terrorism, Crime and Security Act 2001 (ATCSA) (Part 11 thereof). This Act provides for a scheme under which communication service providers would retain ‘communications data’ for specified periods of time, either voluntarily or mandated, for the purpose of safeguarding national security.⁷⁹⁴ While it is difficult to be categorical about it, it may be possible for injured IP owners to rely on data retained under the 2001 Act as evidence in cases against possible infringers.

Section 102, ATCSA requires the Secretary of State to issue a code of practice relating to the retention by communications providers of communications data obtained by or held by them. A Code of Practice⁷⁹⁵ setting out a variety of retention periods for different types of communications data, was laid before Parliament on 11 September 2003. An Order (The Retention of Communications Data (Code of Practice) Order 2003),⁷⁹⁶ bringing the code of practice into, force was made on 5 December 2003.

Section 104 of the 2001 Act empowers the Secretary of State to give directions about the retention of communications data to communications providers generally or particular communications providers. The order must specify the maximum period for which a communications provider may be required to retain the communications data. A sunset provision (contained in Section 105) states that Section 104 will cease to have effect two years after the Act’s passing, but Section 104’s period of operation was extended by the Secretary of State.⁷⁹⁷

⁷⁹⁴ Anti-Terrorism, Crime and Security Act 2001, s 102 et seq.

⁷⁹⁵ Joint Committee on Human Rights, *Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-terrorism, Crime and Security Act 2001* (2002-03, HL 181, HC 1272).

⁷⁹⁶ The Retention of Communications Data (Code of Practice) Order 2003, SI 2003/3175.

⁷⁹⁷ This was done by way of The Retention of Communications Data (Extension of Initial Period) Order 2003, SI 2003/3173, art 2; The Retention of Communications Data (Further Extension of Initial Period) Order 2005, SI 2005/3335, art 2.

7.5 Conclusions

Undoubtedly, one of the chief challenges with online copyright infringements is identifying the tortfeasor. And, if defendant identification cannot occur, for whatever reason, then application of Article 2, Brussels I becomes a dead letter.

In this chapter, we saw that an amalgam of judge-made relief, data retention legislation and technology can potentially assist IP claimants with their task of identifying online defendants.

In terms of the *Norwich Pharmacal* component, the rulings in *Smith v ADVFN* and *Media C.A.T.* are correctives and are, arguably, authority for the proposition that this form of equitable relief will be granted with more circumspection by the courts going forward. Following *Smith v ADVFN*, it looks as if the judiciary will have to carefully consider whether the material complained of is, in fact, defamatory. In addition, if a claimant can obtain the documents from another source or by other means, then the court is unlikely to grant a NPO.

Judge Birss' critical approach to the use of NPOs in *Media C.A.T.* may presage a greater scrutiny of the safeguards governing the use of the information obtained under NPOs. Conscious of certain weaknesses in the system, Birss J used the example of the *Anton Piller* orders to propose the appointment of a neutral supervising solicitor to ensure that the NPO is not abused. This ruling represents a more critical interpretation of *Norwich Pharmacal* relief in which the presiding judge is aware of the real risk of the successful applicants abusing the information disclosed under the order. There is, of course, the possibility that this ruling will act as a catalyst for a complete reappraisal of the *Norwich Pharmacal* jurisdiction. It may well transpire in the future that restrictions will be placed on information disclosed under NPOs and that the granting judge will provide directions on the use of the information disclosed.

Until 8th April 2014 (the date on which the *Digital Rights Ireland* ruling was handed down by the CJEU), the data retention facilitative component seemed to offer considerable assistance to prejudiced rightholders. However, following the CJEU judgment, the situation has become unclear and confused. Importantly, from a rightholder's perspective, the UK's transposing legislation is still part of the law of the land. The Luxembourg ruling has no automatic effect on the relevant national legislation. But, in the light of *Digital Rights Ireland*, the UK may decide to abrogate

the transposing legislation, or, modify it so as to comply with the concerns expressed by the CJEU. Possibly more pertinent still will be the attitude of the UK's ISPs and Telcos. Seeing that the local secondary legislation might well be challenged in domestic courts, the ISPs' erstwhile diligence in retaining data may begin to wane. This would not benefit the position of prejudiced rightholders.

The UK courts will be cognisant of the now impugned EU data retention legal framework. As the Data Retention Directive was declared by the CJEU to be invalid from the date it entered into force, this element of retrospection could potentially undermine, in a serious fashion, many previous court rulings which turned on data evidence. Naturally, UK courts will be very aware of the now impugned EU data retention framework and the element of retrospection. These factors too might make UK courts less inclined to grant NPOs while the legal landscape is so uncertain.

Geolocation technology can provide private international lawyers with considerable assistance when it comes to identification of geographical location on the internet. This has already been demonstrated in the *Yahoo!* and *Gutnick*⁷⁹⁸ cases, where geolocation technology was deployed as an evidential tool. The technology is gradually transforming the internet into a medium that takes account of geographical and legal borders.⁷⁹⁹ Importantly, too, courts have started to take account of geolocation technologies and this development can only have a positive effect. The technology has been acknowledged and endorsed in two US rulings – *National Federation of the Blind v Target Corporation*, and *Hageseth v Superior Court* - along with one German ruling – *VGH Bayern*, 10 CS 08.2399.⁸⁰⁰ As demonstrated earlier in this chapter, geolocation service providers will strive to improve the accuracy of their geolocation technology and this improved accuracy will persuade courts to attach even greater importance to these technologies.⁸⁰¹ According to Olsen and Jacobus, the roll-out of IPv6 should also assist geolocation greatly. Given the clear localisation challenges thrown up by the

⁷⁹⁸ *LICRA, UEJF v Yahoo! Inc, Yahoo France*, Interim Court Order, 20 November 2000, Tribunal de Grande Instance de Paris (Country Court of Paris); *Yahoo!, Inc v LICRA*, 169 F Supp 2d 1181 (ND Cal 2001); *Gutnick v Dow Jones* [2001] VSC 305.

⁷⁹⁹ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 414.

⁸⁰⁰ Handed down 20th November 2008.

⁸⁰¹ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 414.

internet, it would be short-sighted of conflicts lawyers to ignore the potential benefits offered by geolocation technology.

The use of geolocation technology is not problem-free. Doubts remain about the accuracy levels of the technology and there is a growing jurisprudential trend which views IP addresses as personal data. This latter point could place quite serious legal and commercial strictures on geolocation service providers.

On balance, however, geolocation technology constitutes a fillip for both the courts and copyright owners (claimants), a fillip that is likely to grow rather than diminish with the passage of time.

Chapter 8 Jurisdictional Issues: Article 2, Brussels I

Non-facilitative Elements

TABLE OF CONTENTS

8.1	The Objective of the Chapter.....	272
8.2	Tracing Internet Traffic	272
8.2.1	The 'Leasing' or Dynamic Allocation of IP Addresses	276
8.3	Conclusions.....	282

8.1 The Objective of the Chapter

The objective behind this short chapter is to introduce a sense of balance into the analysis of Article 2, Brussels I. While the previous chapter focused on elements facilitative of the operation of Article 2, this chapter focuses on the non-facilitative element of leasing or dynamic allocation of internet protocol (IP) addresses. In other words, it examines a factor that could impede defendant identification. The author acknowledges the non-facilitative nature of anonymising software/techniques but they will not be discussed in any detail in this chapter.

Dynamic allocation of IP addresses is a fact of life, explicable by the aim of making better use of diminishing internet protocol space. From an evidential viewpoint, the dynamic allocation of IP addresses militates against the successful tracing of online copyright infringements.

8.2 Tracing Internet Traffic

It may be possible to identify an online copyright infringer by tracing the internet traffic which relates to the infringing material. If the infringing material had been sent via e-mail, valuable information (from an evidential perspective) will be contained in the e-mail's header. This information will have been provided by the author's computer, intermediate computers through which the e-mail passed, and the recipient's computer.

In most e-mail applications, the e-mail header will be hidden from view but it can be accessed if required. It is the information in the e-mail header that is required to enable the author of the e-mail message to be traced.⁸⁰² The author's ISP will be deducible from the information contained within the header. The author's ISP can then be contacted and provided with a number of elements from the e-mail header which can typically be correlated with the IP address allocation logs and additional logged data, to identify the account that was used to send the message.

Often, considerable resources are dedicated to tracing internet traffic, but investigators will in many instances reach a 'dead end' particularly if the person being traced has the incentive and knowledge to hide his tracks. Even if the trace proves successful, it may

⁸⁰² Craig Earnshaw and Sandeep Jadav, 'E-Mail Tracing' (2004) 15 C & L 8.

not provide the level of forensic reliability to satisfy even the civil standard of proof. This can be explained as follows. First, the IP address often relates to a particular segment of a network rather than to a particular computer. Secondly, in many situations where unlawful behaviour is alleged, it is not sufficient merely to link an individual to a particular computer since a computer is only a tool that can be used by *anyone* having physical access to it or, indeed having *remote access* to it.

As regards the first point in the previous paragraph, it is the MAC address⁸⁰³ which is the immutable identifier linked to a particular piece of hardware, not the IP address. As a general rule, these hardware-encoded addresses are immutable but it must be borne in mind that it is a simple matter to substitute the Network Interface Card (NIC) in a computer with another card for as long as it takes to do whatever it is that one wants to do anonymously. Some networks are configured to deny physical connection to any computer not having a particular MAC address but, on the other hand, very many are not.

Also, a single IP address may mask a range of private IP addresses. IP addresses can be static or dynamic. The significance of the static or dynamic configuration is as follows: If the address is static in the sense that it is an address always given by an ISP to a particular customer, the accounting or the other records of the ISP can be useful evidence in proving that a message from that static address was at least likely to have been sent from that customer's computer. If, on the other hand, the address is dynamically allocated by the ISP's DHCP server it may be almost useless information from an evidential viewpoint. This is because at a time when internet access is often offered at a set monthly charge for unlimited time and volume, there will be no financial incentive for an ISP to keep records of what telephone link or number called from corresponds to any particular IP number within the ISP's allocated range.

As mentioned earlier, the internet works by the packet switching system. Connections are established by a series of 'hops' from one router to another. Fortunately, from the tracer's perspective, it is in the interests of those who run systems representing intermediate 'hops' to keep records of connections to them. This is seldom done to aid traceability of internet traffic. It is more often done for reasons of network or system

⁸⁰³ In addition to having an IP address, each connected device also has a unique 48-bit Media Access Control address or 'MAC'. The MAC is sometimes termed the 'hardware' address.

efficiency, routing efficiency and system security. Nevertheless, there are some positive effects for the tracer.

The ISP will normally keep a series of 'logs' or records about connections, etc. These are created automatically by their server(s). Some logs are configured to collect more complete information about 'callers' as, for example, details of the web browser used or details of 'cookie' files on the calling computer. But, at the very least, it is usual for time-stamped IP source address information to be collected.

The upshot of this is that a message received at its destination should be traceable by one 'hop' at least to the receiver's ISP. At that stage, one begins the difficult task of working backwards: securing any log information retained by that ISP to determine the next hop and so on in the hope that the trail will not be lost. Unfortunately, there is great scope for losing the trail although, at least these days with the move to a more hierarchical routing architecture and geographical allocation of IP addresses, it is much easier to link a particular address with a particular country.⁸⁰⁴ Also, there are still a significant number of IP addresses still being routed that were not allocated according to the new regime and which are not easily amenable to geographical resolution.

One significant problem encountered by tracers is that while ISPs may collect the desired information, they may not keep it for very long.⁸⁰⁵ After all, there is little incentive for them to do so because the information, once it ceases to be of use in terms of monitoring the efficient workings of a particular network, just takes up valuable space and puts considerable strain on their data storage facilities. In fact, there is every

⁸⁰⁴ See <<http://where-is.info/>>.

⁸⁰⁵ After the recent CJEU ruling in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland Ltd v Minister for Communications, and Kärntner Landesregierung*, there will be less incentive for ISPs to retain public electronic communications data for lengthy periods after the EU's most senior court held the Data Retention Directive to be invalid. Admittedly, the implications of this ruling are still being worked out, but the CJEU (at paras 63 and 64 of its ruling) is quite critical of the data retention period contained in the Directive (i.e. minimum of 6 months, maximum of 24 months). The court points out how the retention period is not based on objective criteria. It is also critical of the absence of any distinction being made (in a retention context) between the various categories of data (set out in Article 5 of the Directive) in terms of their possible usefulness for the objective being pursued.

incentive to destroy out-of-date data as soon as possible to avoid being bothered by court-assisted tracers such as LEA.

Another obstacle in the way of tracers is that even if records are kept, they will often be stored in other jurisdictions through which the message has passed. To obtain the logs from these distant relay points will usually involve an application to the court in that particular country. In some countries, internet law has not developed to the point where the local courts have any jurisdiction to assist even if they wanted to. Significantly, online copyright infringers will use this to their advantage.

Anonymous remailers strip out identifying information from IP datagrams. Their policy of offering anonymity means they will not keep log records that would be of any use to a tracer. Moreover, they will often be situated in precisely the jurisdictions that cannot or will not respond in a timely or helpful way to a tracer's requests for assistance.⁸⁰⁶

While it is possible to trace the route a data packet takes on its journey if it has been configured, it would require a potentially large number of individual ISPs (across many jurisdictions) to co-operate and divulge the structure of part of their network, and this may be highly sensitive information. Also, looking at the situation from a very practical point of view, is it really in the interests of an ISP to assist a copyright holder who is alleging copyright infringement?⁸⁰⁷ Countless acts of online copyright infringement are committed every day throughout the world.

⁸⁰⁶ See the discussion of the <anon.penet.fi> anonymous remailer in Paul A Strassman, 'Risk-Free Access into the Global Information Infrastructure via Anonymous Re-mailers' (Symposium on the Global Information Infrastructure: Information, Policy & International Infrastructure, Cambridge, MA, 28-30 January 1996) <<http://www.strassmann.com/pubs/anon-remail.html>> accessed 5 June 2014.

⁸⁰⁷ This voluntary form of ISP assistance should be contrasted with ISPs' legal obligations arising from the E-Commerce Directive. For instance, under Article 13 (the 'caching' provision) of the Directive, the ISP must 'act expeditiously to remove or to disable access to information' (in this case, infringing material) which it has stored upon obtaining actual knowledge of the fact that a court or an administrative authority has ordered such removal or disablement. Similarly, under Article 14 (the 'hosting' provision) of the Directive, the ISP is obliged to 'act expeditiously to remove or disable access to information' that it has stored upon obtaining knowledge or becoming aware of the fact that the information stored is illegal or linked to an illegal activity. Generally speaking, the ISP enjoys immunity under the 'mere conduit' (Article 12), 'caching' (Article 13) and 'hosting' (Article 14) provisions of

8.2.1 *The 'Leasing' or Dynamic Allocation of IP Addresses*

The phenomenon of the 'leasing' of IP addresses⁸⁰⁸ also militates against the successful tracing of online copyright infringements and it has special relevance for the subject of anonymity. Leasing of IP addresses began in the 1990s in an endeavour to make better use of fast diminishing IP space. 'Leasing' is linked to the fact that during the early days of the internet, a large proportion of internet users connected through a dial-up connection with an ISP.⁸⁰⁹ These internet users did not have a permanent connection.

For example, it is clear that if an ISP had one million customers, they could not all be online at the same time. It would have been inefficient to allocate an IP address to each customer. Hence, the number of probable users at any one time was estimated and an equal or greater number of addresses was allocated to a 'pool'. Instead of the connected dial-up host having a 'static' IP address, it had an address allocated dynamically, as

the E-Commerce Directive provided it complies with certain conditions. For example, the ISP enjoys immunity in cases of transmission on a communication network (mere conduit provision) on condition that (a) it does not initiate the transmission; (b) it does not select the receiver of the transmission; and (c) it does not select or modify the information contained in the transmission. In addition, storage by the ISP of information transmitted over its network is legal provided 'the information is not stored for any period longer than is reasonably necessary for the transmission' (Article 12(2)).

⁸⁰⁸ The phrase 'leasing of IP addresses' is used by Chris Nicoll, 'Concealing and Revealing Identity on the Internet' in C Nicoll, JEJ Prins and MJM van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions - Information Technology & Law Series 2* (1st edn, Asser Press 2003) 104.

⁸⁰⁹ Broadband internet access (cable and DSL) soon began to eclipse dial-up connections thanks to significantly higher connection speeds. In 2008, a Pew Internet and American Life Project study found that only 10% of American adults still used dial-up internet access. Some of the reasons for retaining dial-up access were lack of infrastructure and high broadband prices. Sometimes, ISPs refused to roll-out high speed internet due to fears about profitability and costs associated with building infrastructure. Interestingly, from 2009 on, as the global recession took hold, a resurgence in dial-up access occurred in the US. This trend is linked to pricing with the standard dial-up package sometimes costing almost 60 per cent less (per month) than the standard DSL and Cable package.

needed, from that pool by a service such as DHCP⁸¹⁰ or BOOTP.⁸¹¹ The DHCP service was run by the ISP's logon server when the dial-up connection was made.

A valid IP address was then given to the customer. When the customer disconnected, his address was returned to the pool so that it would be available for another customer. There were implications for anonymity as the IP address used by a particular customer while online was of little use in tracing the origin of a message because there was no administrative link between the customer's identity and the IP address used by that customer – his address was commonly allocated at random. The challenge presented by dynamic allocation of IP addresses has also arisen in the investigation of online paedophilic activity.⁸¹²

A good example of a ruling concerning dynamic allocation of IP addresses is the Canadian judgment, *BMG Canada Inc v John Doe*,⁸¹³ is instructive in relation to the dynamic nature of most IP addresses.⁸¹⁴ A motion was brought by members of Canada's

⁸¹⁰ The Dynamic Host Configuration Protocol. For example, to determine whether an IP address is dynamic or static on a Microsoft Windows workstation, one must view the selected TCP/IP options in <Control Panel><Network>.

⁸¹¹ Christian Czychowski and Jan Bernd Nordemann, 'Use of Retained Data and Copyright Law in Germany – the German Data Protection Problem to Fight Internet Piracy' (2010) 32 EIPR 174, where it is stated that internet access providers generally do not ascribe non-corporate clients a permanent IP address. Instead, these receive a so-called dynamic IP address that renews itself each time the user logs onto the internet. This dynamic IP address can generally be ascertained by third parties. The identity of the client, however, remains anonymous. The client can only be traced by the provider consulting client data to determine who was ascribed the relevant dynamic IP address at the time of the infringement. Without the provider consulting this data, the identity of the copyright infringer cannot be ascertained and the infringement, be this criminal or civil infringement of copyright, cannot be pursued.

⁸¹² See Matthieu Latapy, Clémence Magnien and Raphaël Fournier, 'Technical Report on Quantification of Paedophile Activity in a Large P2P System' (2009) 7 <<http://antipaedo.lip6.fr/T24/TR/quantification.pdf>> accessed 4 July 2012.

⁸¹³ *BMG Canada Inc v John Doe* [2004] FC 488.

⁸¹⁴ For a more recent account of dynamic allocation of IP addresses see the 2013 Irish Supreme Court ruling in *EMI Records (Ireland) Limited v Data Protection Commissioner* [2013] IESC 34 [3.6] where the following is stated (in the context of Ireland's Graduated Response Protocol):

recording industry seeking disclosure from five Canadian ISPs⁸¹⁵ of the identity of certain customers who, it was alleged, had infringed copyright laws by illegally trading in music downloaded from the internet.⁸¹⁶ The following passage is taken from para 19 of the judgment:

Because the frequency of visits and duration of time spent online differs from user to user, the IP addresses are not assigned to the MAC addresses sequentially. As a result of this functionality, IP addresses are not associated with any one account holder nor are they allocated in any predetermined pattern (the use of the term 'IP address' is perhaps confusing in the conventional sense because it is not an address, as one understands a house to have an address). It is therefore not possible to directly identify an account holder merely from an IP address. Moreover, searching for the IP address is not straightforward.

The affidavits filed by the five ISPs reveal that it is not an easy task to provide the name and address of the account holder who used a specific IP address at a given time.⁸¹⁷ At

The IP address of any particular subscriber is allocated typically on a daily basis by an ISP, so that a user will have a different IP address from one day to the next. The record companies, through their agents, receive IP addresses of internet users who have allegedly uploaded material to the internet where the intellectual property rights of such material belongs to the record companies. The record companies or their agents cannot identify the alleged wrongdoer as they cannot link the IP address to any individual subscriber. The record companies, therefore, communicate this information and the respective IP addresses to Eircom who do have the ability to link the allegedly offending IP addresses with the appropriate subscribers.

⁸¹⁵ Shaw Communications Inc, Rogers Cable Communications Inc, Bell Sympatico, Telus Inc and Vidéotron Ltée.

⁸¹⁶ The plaintiffs are unable to determine the name, address or telephone number of the 29 Internet users in question as they operate under pseudonyms associated with software which they use, eg Geekboy@KaZaA. However, they conducted an investigation through which they submit, it was discovered that these individuals used Internet Protocol addresses (IP addresses) registered with the ISPs which are the respondents to this motion. *BMG Canada Inc v John Doe* [2004] FC 488 [2].

⁸¹⁷ Similarly, where a block of IP addresses has been allocated by an ISP to a subscriber who provides either anonymous public services (cyber café) or, does not maintain a historical log

para 33 of the judgment, reference is made to the contents of an affidavit filed by one of the TELUS employees. In this affidavit, the employee describes the process as follows:

To attempt to obtain that information requested, TELUS employees will be required to conduct searches of at least three different databases and cross-reference the information found, to locate the likely account holder. This process is not done in the normal course of business and thus there are no existing lists, files, records, or documents containing the information requested. In addition, none of the TELUS staff would know the information requested as a result of their normal duties. TELUS does not monitor the content of what account holders access on the Internet.⁸¹⁸

The only way to locate the account that accessed the Internet using the IP address in question would be to cross-reference the IP address at the date, time, network and time zone to a database of MAC addresses and then cross-reference the MAC address with the account database, assuming that the information still exists and is recoverable. As discussed below, the more historic a search is, the less reliable the information will be, as records are kept in different ways for different systems.⁸¹⁹

The TELUS employee goes on to aver in his affidavit how difficult it is for an ISP to identify a user of its services and he emphasises the importance of the prejudiced copyright holder (or other requester) lodging a request with an ISP soon after an online copyright infringement is suspected.

Please note that TELUS can never identify the 'user', ie, the person actually using the computer at the time of the alleged infringement. TELUS can only identify the person who opened up the TELUS account associated with the MAC address. As will be discussed below, the account holder and the user are not always the same, or even known to each other. With respect to the account holder, if the request is made within 30 days of when the internet was accessed

of IP address allocation, it will be very difficult to match the IP address to a specific user. Ian Walden 'Forensic Investigations in Cyberspace for Civil Proceedings' (2004) 18 Int'l Rev L Computers Tech 275, 276.

⁸¹⁸ *BMG Canada Inc v John Doe* [2004] FC 488 [33] sub-para 16.

⁸¹⁹ *Ibid* sub-para 17.

for the peer-to-peer sharing activity, TELUS has a good chance of identifying the account (depending on the particular TELUS internet system the customer was using). However, for requests concerning customer activity 30 days or more before the request, the information becomes less reliable to the point of being non-existent.⁸²⁰

While the TELUS employee refers to a 30 day period, others would argue that in the case of e-mails (transmitting infringing material), the ISP ought to be contacted within 14 days of the mail passing through/being received at its servers. This is because the IP address allocation logs and other relevant logged data are typically only stored by the ISP for a fortnight.⁸²¹ An important distinction should also be drawn between the dynamically allocated IP addresses, usually employed in the case of home users or small businesses and, static IP addresses, often owned or leased (on a long-term basis) by corporate users and which do not change over time.

In *BMG*, the plaintiffs' motion requiring the defendant ISPs to disclose their customers' identities was dismissed by the Federal Court. The court justified its decision by the fact that the plaintiff music companies failed to limit acquisition of information to copyright infringement issues.

On appeal to the Federal Court of Appeal,⁸²² the appellants (plaintiffs) once again failed in their bid to obtain an order under Federal Courts Rules, 1998,⁸²³ rr 233, 238 to compel the ISPs to disclose names of customers who allegedly infringed copyright online. The appellants' case was weakened by the fact that much of their evidence was hearsay, thereby failing to comply with rule 81 (of the Federal Courts Rules, 1998) which requires affidavits to be confined to personal knowledge. Privacy considerations were important in the appeal hearing. In essence, the Court of Appeal decided that for a disclosure order to be made against the ISPs, the public interest in favour of disclosure would have to outweigh the legitimate privacy concerns of the ISPs' customers. This delicate balance between privacy interests and the public interest would have as its backdrop the Personal Information Protection and Electronic Documents Act (PIPEDA)

⁸²⁰ Ibid sub-para 22.

⁸²¹ Craig Earnshaw and Sandeep Jadav, 'E-Mail Tracing' (2004) 15 C & L 9.

⁸²² *BMG Canada Inc v John Doe* [2005] FCA 193.

⁸²³ Federal Courts Rules, SOR/98-106, Federal Courts Act, Rules for Regulating the Practice and Procedure in the Federal Court of Appeal and the Federal Court.

2000 which prohibits ISPs from voluntarily disclosing personal information such as identities requested except with the customer's consent or pursuant to a court order.

However, even with static IP addresses, a company can enable multiple computers on a network to utilise the same IP address (via Network Address Translation). With this service, each computer can still uniquely request and receive information from the internet: a computer on the corporate network is used to perform a 'translation' between the internal, private address that each computer on the network is allocated, and the external, public IP address that enables data on the internet to be accessed.⁸²⁴ Given the more stable character of the static IP address system, it might be easier for prejudiced copyright owners (or some entity on his behalf) to trace the originating computer provided assistance were provided in terms of the Network Address Translation.

The inescapable conclusion is that it is seldom, if ever, possible to trace a datagram encapsulated using IPv4 where the sender is determined to avoid tracing and has taken various simple precautions to remain undetected and hence anonymous. For instance, there are a number of software applications, online re-mailing and anonymising services⁸²⁵ and other more advanced techniques that can be used to obfuscate an individual's IP address, thereby potentially preventing it from being traced.⁸²⁶ Alternatively, a successful IP spoofing attack⁸²⁷ on a system that is insufficiently protected may provide a suitable springboard to attacking other systems.

⁸²⁴ Craig Earnshaw and Sandeep Jadav, 'E-Mail Tracing' (2004) 15 C & L 7 et seq.

⁸²⁵ Effected via an intervening anonymising server often located in an 'inhospitable' jurisdiction.

⁸²⁶ Craig Earnshaw and Sandeep Jadav, 'E-Mail Tracing' (2004) 15 C & L 9.

⁸²⁷ Spoofing occurs when a hacker logs in to a computer under a different identity. This will be possible if the hacker has previously obtained actual passwords, or has created a new identity for himself by fooling the computer into thinking he is the system's operator. Clive Gringras and Elle Todd, *Gringras: The Laws of the Internet* (3rd edn, Tottel 2008) 339, para 5.6.2.1.2., 237. IP Spoofing can take place because authenticated communication between two computers occurs solely on the basis of their respective IP addresses. For example, a person may login to a remote UNIX system without any form of username or password verification provided (a) the 'rlogin' service is activated on the remote system and (b) the login originates from a computer which appears to have an 'approved' IP address. As a practical matter, 'approval' is achieved by the system administrator's listing the IP address of the remote computer in the target computer's '.rhosts' file. If the target computer is fooled into

It also has to be said that a successful trace using the IP address leads the tracer to a computer – not necessarily to the user of that computer!⁸²⁸ However, further action could be taken by the tracer on the basis of this information. For instance, the tracer could seek an order for the delivery up of the computer(s) that are configured with the name of the computer showing up in the trace results. Tracing involves establishing the beginning and the end of one or more 'hops'. Such 'hops' often span different countries and, hence, different jurisdictions. To be investigated properly they depend on the availability of records kept by independent third parties who are seldom interested in the dispute under investigation.

While the courts in some countries will assist in obtaining the necessary access where it appears unlawful activity has taken place, the transnational nature of much online IPR infringement will often frustrate the investigation insofar as these remedies are not universal or consistently applied.⁸²⁹

8.3 Conclusions

As regards the dynamic allocation of IP addresses, *BMG Canada v John Doe* demonstrates how IP addresses are not assigned to the MAC addresses sequentially. Accordingly, IP addresses are not associated with any one account holder nor are they allocated in any predetermined pattern. Consequently, it is not possible to directly identify an account holder merely from an IP address. Evidence adduced by the ISP's

thinking the originating computer bears the approved IP address serious damage can be caused to the target and the perpetrator can remain anonymous. Indeed, once the perpetrator gains access to the target, he can use it as a springboard to other systems – particularly those that 'trust' the target. Chris Nicoll, 'Concealing and Revealing Identity on the Internet' in C Nicoll, JEJ Prins and MJM van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions - Information Technology & Law Series 2* (1st edn, Asser Press 2003) 106 et seq.

⁸²⁸ The account details that are provided by the ISP may not necessarily be indicative of the author of the e-mail in question, as they will only record the contact details of the individual who opened the account with the ISP. Craig Earnshaw and Sandeep Jadav, 'E-Mail Tracing' (2004) 15 C & L 9.

⁸²⁹ The information contained in the sections on Tracing Internet Traffic is derived from Chris Nicoll, 'Concealing and Revealing Identity on the Internet' in C Nicoll, JEJ Prins and MJM van Dellen (eds), *Digital Anonymity and the Law: Tensions and Dimensions - Information Technology & Law Series 2* (1st edn, Asser Press 2003) 116-119.

employees revealed that the task of linking a name and address of an account holder to a specific IP address is far from straightforward and would involve cross-referencing the IP address to a database of MAC addresses and then cross-referencing the MAC address with the account database. To compound problems, the more historic the search, the less reliable the information. It seems that requests relating to customer activity which is at least 30 days old are highly likely to be unreliable.

Chapter 9. Jurisdictional Issues

–

Article 5 (3), Brussels I

TABLE OF CONTENTS

9.1	Introduction.....	285
9.2	Article 5(3), Brussels I	285
9.2.1	The New Wording of Article 5(3), Brussels I and Challenges for Conflicts Lawyers	287
9.3	Establishing the Locus of the Tort – the 2002 Dow Jones v Gutnick ruling 288	
9.3.1	Dow Jones & Company Inc v Gutnick.....	288
9.3.2	Implications of the ruling	295
9.3.3	Jurisprudential inconsistency, post-Dow Jones	296
9.3.4	English rulings which followed the Gutnick Approach	297
9.3.5	The Defamation Act 2013	299
9.3.6.	The Ministry of Justice’s Consultation Paper	301
9.4.	Conclusions	301

9.1 Introduction

Following on from my analysis of both facilitative and non-facilitative elements in the context of Article 2, Brussels I, in chapters 7 and 8, I shall now turn to the other important jurisdictional provision within Brussels I, namely Article 5(3). This is a special jurisdictional rule, applying to torts, delicts and semi-delicts.

This chapter has two objectives. They are:

1. To demonstrate how the new wording of Article 5(3), Brussels I, by providing for prospective torts and *quia timet* proceedings, creates difficulties for conflicts lawyers. Arguably, under the revised wording of Article 5(3), there is now a triality of jurisdictional possibilities open to the plaintiff (claimant).
2. Using the analogue of online defamation, determine how the courts have interpreted the issue of *locus delicti* in such situations.

9.2 Article 5(3), Brussels I

Article 5(3) of Brussels I constitutes another possible jurisdictional route for the plaintiff copyright holder. It is an exception to the basic jurisdictional rule (contained in Article 2) and provides the plaintiff with an alternative to suing in the courts of the place of the defendant's domicile. Under Article 5(3), the plaintiff can sue in a number of different fora - in the place where the tort occurred or in the place or places where the tort *may occur*. This new jurisdictional possibility was introduced under Brussels I when the wording of Article 5(3) of the Brussels Convention was changed to the effect that the words 'or may occur' were added to the end of that particular provision. Article 5(3) now reads as follows:

A person domiciled in a Member State may, in another Member State, be sued 'in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur.'

Arguably, the effect of the 'new' Article 5(3) creates three distinct connecting factors, namely, the place where the harmful event (damage) occurred, the place of the event giving rise to the harmful event (damage) and the place where the harmful event *may*

occur. Under the *Bier* formula,⁸³⁰ a duality of jurisdiction existed whereby the plaintiff could sue the defendant in either the jurisdiction where the damage occurred or in the jurisdiction where the event giving rise to the damage occurred.⁸³¹ Following the change in wording of Article 5(3), this duality has now become a triality!

I will now examine the application of Article 5(3) to an online situation. In applying Article 5(3) however, we will first have to assume that the defendant has already been identified (a not altogether easy task) and the plaintiff has opted not to sue (under Article 2) in the courts of the place where the defendant is domiciled. If the plaintiff is going to invoke Article 5(3), he must decide where he is going to institute proceedings. In essence, he can sue in the Member State where his copyright has been infringed or in the Member State or Member States where he believes his copyright may, at some future time, be infringed.

Given the instantaneous and simultaneous nature of the internet, it is of course possible that the copyright holder's rights be infringed in a number of different jurisdictions at the same time or within a very short space of time. The new wording of Article 5(3)

⁸³⁰ The *Bier* ruling is analysed at para 4.2.3.2.

⁸³¹ This dual approach has been applied, or at least acknowledged, by the European Court of Justice in matters, ia of water pollution (Case 21/76 *Handelskwekerij G J Bier BV v Mines de Potasse d'Alsace SA* [1976] ECR 1735, para 24); liability of a maritime carrier (Case C-51/97 *Réunion Européenne SA v Spliethoff's Bevrachtingskantoor BV* [1998] ECR I-6511, para 32); defamation through a newspaper article (Case C-68/93 *Fiona Shevill, Ixora Trading Inc, Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-415, paras 20, 23); wrongful industrial action of a trade union (Case C-18/02 *Danmarks Rederiforening, acting on behalf of DFDS Torline A/S v LO Landesorganisationen I Sverige, acting on behalf of SEKO Sjöfolk Facket för Service och Kommunikation* [2004] ECR I-1417, para 40); liability of investment consultants (Case C-168/02 *Rudolf Kronhofer v Marianne Maier* [2004] ECR I-6009, para 16). In *Réunion Européenne SA v Spliethoff's Bevrachtingskantoor BV*, the ECJ noted that there may be cases of international transport operations where 'the place where the event giving rise to the damage occurred may be difficult or indeed impossible to determine', in which case Article 5(3) would only allocate jurisdiction to the place where the damage occurred. In addition, the court stated that the place where damage occurred could not be either the place of final delivery (which can be changed mid-voyage) or the place where damage was ascertained. Case C-51/97 *Réunion Européenne SA v Spliethoff's Bevrachtingskantoor BV* [1998] ECR I-6511, para 33.

would cover onward transmission of works. This occurs where a digital work is illegally copied and sent to a third party, in exchange for payment. This would amount to a commercialisation of the work, thereby constituting a secondary infringement of copyright. If the infringing work is transmitted onwards, it may be used by someone who knows that it is infringing material.

As regards analysis of the term 'harmful event', the first step involves working out what the term means in the context of copyright infringement. Since copyright actually comprises a bundle of rights,⁸³² infringement by the copyright pirate of any one or more of these constituent rights would probably qualify as a 'harmful event'.

9.2.1 The New Wording of Article 5(3), Brussels I and Challenges for Conflicts Lawyers

The addition, under Brussels I, of the words 'or may occur' to Article 5(3)⁸³³ creates an unclear situation for conflicts lawyers and especially for those dealing with conflicts in an online context. The simple truth is that copyright infringements, whether committed online or offline, may occur anywhere in the twenty-eight Brussels I States.⁸³⁴

⁸³² See para 6.3

⁸³³ In the October 2002 ruling in *Verein für Konsumenteninformation v Karl Heinz Henkel*, the European Court of Justice, when interpreting Article 5(3) of the Brussels Convention 1968, ruled that said provision covers actions which seek to *prevent* the occurrence of damage. Case C-167/00 *Verein für Konsumenteninformationen v Karl Heinz Henkel* [2002] ECR I-8111, paras 44-48. See also ruling of the ECJ in Case C-18/02 *Danmarks Rederiforening, acting on behalf of DFDS Torline A/S v LO Landesorganisationen I Sverige, acting on behalf of SEKO Sjöfolk Facket för Service och Kommunikation* [2004] ECR I-1417, paras 27-34. For a Scottish ruling confirming that Article 5(3) applies to threatened delicts as well as to completed delicts see *Bonnier Media Ltd v Smith; sub nom Bonnier Media Ltd v Kestrel Trading Corp* [2002] SCLR 977 [12]. This case involved allegations of the use of a business domain name with the aim of passing off as other organisations.

⁸³⁴ Brussels I applies to all Member States of the EU including Denmark. While Brussels I is not directly applicable to Denmark, it has effectively been extended to Denmark by a separate agreement between the EU and Denmark (Agreement between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2005] OJ L299/62) which took effect on 1 July 2007.

The instantaneous nature of the internet combined with the ease with which near-perfect illegal digital copies can be created online, makes the new wording of Article 5(3) all the more problematical for private international lawyers. The addition of the words 'or may occur' to Article 5(3) will have greater consequences for online IP infringement than for offline IP infringement. This is linked to the significantly greater potential for infringing online than offline, given such factors as the truly global reach of the internet and the exponential character⁸³⁵ of online IP infringement. By way of example, an illegal copy of a book remains just one copy even if it is sent from one country to the next. By contrast, an illegal digital copy of a work, if posted online, may be replicated with considerable ease by a large number of internet users and then further disseminated across national borders. In turn, recipients of such work may further disseminate or make new changes and then disseminate. Together, digitisation and the medium of the internet, facilitate wholesale IP theft which is frequently trans-border in character.

9.3 Establishing the Locus of the Tort – the 2002 *Dow Jones v Gutnick* ruling

In attempting to establish where the act of illegal copying takes place, one may have to proceed by way of analogy since precedents in the area of online copyright are relatively rare. It may prove beneficial to examine the act of publication and some of the case law on the issue, arising from the Australian High Court ruling *Dow Jones & Company Inc v Gutnick*⁸³⁶ which involved online defamation.

9.3.1 *Dow Jones & Company Inc v Gutnick*

In *Dow Jones & Company Inc v Gutnick*,⁸³⁷ the Court had to consider two opposing points of view relating to alleged online defamation. The question before the court was

⁸³⁵ By 'exponential', the author is referring to the almost domino-like effect that online infringement creates. By introducing one illegal digitised copy onto the Internet, the copyright pirate is almost ensuring that the infringing copy will be replicated manifold times and disseminated far and wide to be re-copied and re-transmitted to other online users, or possibly just posted on bulletin boards for further anonymous, unauthorised use.

⁸³⁶ *Dow Jones & Company Inc v Gutnick* [2002] HCA 56.

⁸³⁷ *Ibid.*

whether the online publication occurred in the jurisdiction where the article was downloaded or in the jurisdiction where it was uploaded onto a server.⁸³⁸

Mr Joseph Gutnick, a prominent businessman, with a reputation in philanthropic, sporting and religious circles was an international entrepreneur with substantial connections in the US. Gutnick resided and had business headquarters in the Australian State of Victoria. He brought proceedings against Dow Jones, the printers and publishers of the Wall Street Journal, Barron's newspaper and operators of WSJ.com. Gutnick contended that the article 'Unholy Gains' appearing on Barron's online edition (28th October 2000) defamed him and he sought damages in Victoria.⁸³⁹

Dow Jones, invoking the principle of *forum non conveniens*,⁸⁴⁰ argued that the Australian courts did not have jurisdiction. They further contended that jurisdiction

⁸³⁸ This analysis should be contrasted with the analysis in the 'Cristal' case (*Castellblanch SA v Champagne Louis Roederer SA* [2004] IL Pr 41). In that case, the court had to determine where the causal event occurred in the context of an online trademark infringement. The court opted for the place of upload (by the infringer) rather than the place of download. Stated differently, the court ruled that for the purpose of the application of Article 5(3), the causal event is located at the place where the alleged infringer has its establishment. A parallel could be drawn between the aforementioned solution and the approach used in the Satellite Broadcasting and Cable Retransmission Directive, which defines the act of broadcasting as 'the act of introducing the programme-carrying signals in the chain of communication'. Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15, art 1(2)(b); Arnaud Nuyts, 'Suing at the Place of Infringement: The Application of Article 5(3) of Regulation 44/2001 to IP Matters and Internet Disputes' in Arnaud Nuyts (ed), *International Litigation in Intellectual Property and Information Technology* (Kluwer Law International 2008) 121.

⁸³⁹ The reasons for doing so were recorded by the primary judge that he 'is indifferent to the other substantial parts of the article and desires only that the attack on his reputation in Victoria as a money-lauderer should be repelled and his reputation re-established.' *Dow Jones & Company Inc v Gutnick* [2002] HCA 56 [6]; Campbell Deane, 'Jurisdiction and Online Publishing' (2002) 8 Comms L 237.

⁸⁴⁰ Under the doctrine of *forum non conveniens*, the court has a discretion in cases involving both natural and legal persons to stay proceedings if the defendant is able to show that there is another more appropriate forum. The basis of the doctrine is appropriateness rather than simply convenience.

should vest in the US courts since the article on Barron's online was published in South Brunswick, New Jersey, where it was available on servers maintained by Dow Jones.

The Australian High Court stated that the principal issue in the case, which was relevant to all three challenges mounted by Dow Jones was where the allegedly defamatory statement had been 'published'. This inquiry stemmed from the fact that the law to be applied to the case was the law of the country where the tort occurred – the *lex loci delicti*. If it were deemed to have been committed in Victoria, Victorian law would govern the case and there would be a basis for jurisdiction in Victoria and a compelling reason to dismiss Dow Jones' inconvenient forum claim. Dow Jones argued that the law of New Jersey should apply to the case, as it was in that state that the Dow Jones server uploaded the offending article onto the World Wide Web. In fact, there was no relevant connection to New Jersey apart from the presence of the server. Dow Jones was neither incorporated in nor maintained its principal offices in New Jersey. Rather, the company was incorporated under the laws of Delaware and had its main office in New York.⁸⁴¹

Determining the place of publication was of crucial importance, as the law of defamation in Victoria is substantially different from that of New Jersey.⁸⁴² In *Dow Jones*, the place of publication, the defamatory act and damage to reputation were intertwined. Harm to reputation, however, is the gravamen of Australian defamation law. The High Court in *Dow Jones* ruled that damage is done when a defamatory publication is comprehended by the reader, the listener or the observer.⁸⁴³ Chief Justice Gleeson reasoned as follows:

⁸⁴¹ Richard L Creech, 'Dow Jones and the Defamatory Defendant Down Under: A Comparison of Australian and American Approaches to Libellous Language in Cyberspace' (2004) 22 *JMarshall JComputer & InfoL* 553, 556, fn 9.

⁸⁴² In both Australia and the US, the law of defamation is controlled by state law, and within each country the law varies from state to state in many, sometimes significant ways. Putting domestic variation aside, however, even more pronounced differences are evident when Australian defamation law is compared to American law. *Ibid* 556.

⁸⁴³ *Dow Jones & Company Inc v Gutnick* [2002] HCA 56 [26]. On the point of allegedly defamatory material being in comprehensible form, see Raymond SR Ku and Jacqueline Lipton, *Cyberspace Law – Cases and Materials* (3rd edn, Wolters Kluwer 2010) 92 et seq where they state:

It is only when the material is in comprehensible form that the damage to reputation is done and it is damage to reputation which is the principal focus of defamation,

In the case of material on the World Wide Web, it is not available in comprehensible form until downloaded onto the computer of a person who has used a web browser to pull the material from the web server. It is where that person downloads the material that the damage to reputation may be done. Ordinarily, then, that will be the place where the tort of defamation is committed.⁸⁴⁴

Dow Jones' argument that New Jersey should be deemed the place of publication, to the exclusion of all other places was driven heavily by the so-called 'single publication rule', which is a peculiar rule of American defamation jurisprudence, created to deal with widely disseminated publications such as books and newspapers, and later radio and TV broadcasts.⁸⁴⁵ Originally under common law, one could say that if one thousand copies of a defamatory article were made and distributed to one thousand different people, there have been one thousand different publications, and a plaintiff would have one thousand different claims against the defendant. Naturally, this could make the litigation of defamation claims rather complicated especially when publication had occurred in multiple jurisdictions. To simplify matters, American courts developed the single publication rule, which provides that any single edition of a book, newspaper, or so forth, is deemed to constitute a 'single publication', and a plaintiff is allowed only one action to recover damages for that publication. In that single action, however, he may recover all damages suffered in all jurisdictions.⁸⁴⁶ The single publication rule is followed in at least 27 US states, including New Jersey, and it has been held applicable to defamatory publications on the Internet.⁸⁴⁷

not any quality of the defendant' s conduct. In the case of material on the World Wide Web, it is not available in comprehensible form until downloaded onto the computer of a person who had used a web browser to pull the material from the web server.

⁸⁴⁴ *Dow Jones & Company Inc v Gutnick* [2002] HCA 56 [44] (Gleeson CJ).

⁸⁴⁵ The single publication rule was codified as the Uniform Single Publications Act in 1952 and was intended to address the shortcomings inherent in the common law 'multiple publication rule' which allowed numerous and stale lawsuits to stem from a single defamatory statement.

⁸⁴⁶ Richard L Creech, 'Dow Jones and the Defamatory Defendant Down Under: A Comparison of Australian and American Approaches to Libellous Language in Cyberspace' (2004) 22 *JMarshall JComputer & InfoL* 553, 558.

⁸⁴⁷ The rule was first held to be applicable in internet scenarios in *Firth v State of New York*, 706 NYS 2d 835, 841 (2000). This view was maintained in a line of subsequent rulings ie *Van*

On the basis of the single publication rule, Dow Jones argued that what was determinative in the case was its own act of placing the article on a server in New Jersey, which constituted a single act of publication, and not the reading of the article in multiple jurisdictions around the world. Under the single publication rule, Gutnick could only bring one action against Dow Jones to recover all damages for injury to his reputation and, Dow Jones contended, Victoria was an inappropriate place to litigate all such claims, especially when, in its view, it was the law of New Jersey which was to apply to the case.

Significantly for Dow Jones, however, the single publication rule is not a legal doctrine followed in Australia. Instead, the Australians apply the multiple publication rule, sometimes termed the rule in *Duke of Brunswick v Harmer*,⁸⁴⁸ or the repeat publication rule. This rule states that each communication of defamatory matter to a publishee is, in law, a separate publication. The rule has implications for limitation purposes as time will start to run again whenever the defamatory matter is communicated afresh. This poses special difficulties for defendants who publish material on the internet, which may remain accessible for many years after it was first made available.⁸⁴⁹

In *Gutnick*, the consequences of this were that where publication of defamatory material occurred in each Australian state and territory, then each publication constituted a separate actionable wrong,⁸⁵⁰ a principle which stems from Australia's concern with an individual's right to his reputation and his interest in vindicating it wherever it is assailed.

Buskirk v New York Times Co, No 99 Civ 4265 (MBM), 2000 WL 1206732; 28 Media L Rep 2525 (SDNY 2000); 325 F 3d 87 (2nd Cir 2003); *Mitan v Davis*, 243 F Supp 2d 719 (WD Ky 2003); *The Traditional Cat Association v Gilbreath*, 13 Cal Rptr 3d 353, 359 (Cal Crt App 2004).

⁸⁴⁸ *Duke of Brunswick v Harmer* [1849] 14 QB 185.

⁸⁴⁹ As for the multiple publication rule and its effect on the internet, see Brian Neill et al, *Duncan and Neill on Defamation* (3rd edn, LexisNexis Butterworths 2009) para 8.07.

⁸⁵⁰ Clearly the application of the rule in *Duke of Brunswick v Harmer* in the context of internet libel puts the libeller in a very precarious position as he is potentially vulnerable to multiple actions in different jurisdictions. This rule was considered in *Lewis v King* where it was observed that the High Court of Australia (in *Dow Jones v Gutnick*) 'firmly rejected a challenge in the context of internet libel, to the applicability of such established principles as that vouchsafed in *Duke of Brunswick*'. *Lewis v King* [2004] EWCA Civ 1329 [29] et seq.

Dow Jones argued strenuously that the High Court should reformulate Australian defamation law so as to incorporate the single publication rule, and to designate the location of the server as the place of single publication.⁸⁵¹ It further contended that the advent of the internet was a sufficiently revolutionary technological advancement so as to warrant a reconsideration of the law governing the elements of the tort of defamation.⁸⁵² As regards the place of wrong for choice of law purposes, Dow Jones argued that this should be ascertained by reference to where in substance the cause of action arose. In the appellant's view, the cause of action arose in either New Jersey or New York.⁸⁵³

The Australian High Court found numerous problems with this submission. Kirby J was of the view that where a person or corporation publishes material which is potentially defamatory of another, it is not too excessive a burden to ask the publisher(s) to be cognisant of the defamation laws of the place where the person resides and has his reputation.⁸⁵⁴ Callinan J used the analogy of multinational business and pointed to the manufacturers of popular brands of motor car. He pointed out that where they wish to sell their cars abroad, they are obliged to comply with the laws and standards of those jurisdictions.⁸⁵⁵ He continued and used the example of people wishing to do business in or indeed travel to, or live in, or utilise the infrastructure of different countries. In such situations, he noted, they could hardly be absolved from compliance with the laws of those countries.⁸⁵⁶ Later in his ruling, Callinan J highlighted the risk involved for someone who publishes in a multiplicity of jurisdictions. In short, that person must understand and accept that he runs the risk of liability in those jurisdictions in which the publication is not lawful and inflicts damage.⁸⁵⁷

Interestingly, two years prior to the *Dow Jones* ruling, the US District Court in New Jersey held in a case involving alleged trademark infringement that it was unreasonable to subject a defendant to jurisdiction in New Jersey merely because the defendant's

⁸⁵¹ *Dow Jones & Company v Gutnick* [2002] HCA 56 [109] (Kirby J).

⁸⁵² *Ibid* [77].

⁸⁵³ *Ibid* [109].

⁸⁵⁴ *Ibid* [151].

⁸⁵⁵ *Ibid* [186] (Callinan J).

⁸⁵⁶ *Ibid*.

⁸⁵⁷ *Ibid*.

Web server was located in that state.⁸⁵⁸ Curiously, the Australian High Court did not appear to be aware of the New Jersey decision but it is clear from the New Jersey holding that courts on both sides of the Pacific view the location of a server to be a rather flimsy basis for asserting jurisdiction.⁸⁵⁹

In arguing against vesting jurisdiction in the place where the server is located, Kirby J noted that 'the place of uploading of material onto the internet might bear little or no relationship to the place where the communication was composed, edited, or had its major impact.'⁸⁶⁰ The court also expressed concern that if the location of a server determined the law to be applied in a case publishers would be free to manipulate the uploading and location of data so as to insulate themselves from liability in Australia or elsewhere, for example, by using a Web server in a 'defamation free jurisdiction' or one in which the defamation laws are tilted decidedly towards defendants.⁸⁶¹ The court was also cognisant of the fact that a vastly disproportionate share of all of the Web servers in the world are in the US. A rule which would focus on the location of the Web server would greatly extend the reach of American law. Callinan J even went so far as to decry Dow Jones' attempt to impose an American legal hegemony where the consequence:

would be to confer upon one country, and one notably more benevolent to the commercial and other media than (Australia is), an effective domain over the law of defamation, to the financial advantage of publishers in the United States, and the serious disadvantage of those unfortunate enough to be reputationally damaged outside the United States.⁸⁶²

Despite Dow Jones' contention that US law should apply due to the fact that the allegedly defamatory material was made available (uploaded) on servers and therefore published in New Jersey, the Australian High Court rejected that argument.⁸⁶³

⁸⁵⁸ *Amberson Holdings LLC v Westside Story Newspaper*, 110 F Supp 3d 332 (DNJ 2000).

⁸⁵⁹ Richard L Creech, 'Dow Jones and the Defamatory Defendant Down Under: A Comparison of Australian and American Approaches to Libellous Language in Cyberspace' (2004) 22 *JMarshall JComputer & InfoL* 553, 560.

⁸⁶⁰ *Dow Jones & Company Inc v Gutnick* [2002] HCA 56 [130] (Kirby J).

⁸⁶¹ *Ibid* [199] (Callinan J).

⁸⁶² *Ibid* [200] (Callinan J).

⁸⁶³ On the issue of publication, it is worth noting the views expressed by Hedigan J in the lower court, i.e. the Supreme Court of Victoria. He felt that the browser request (from Australia)

Instead, it localised the online defamation at the place where damage to reputation occurred.⁸⁶⁴ Ordinarily, the *locus* of damage will be the place where the alleged defamatory material is available in comprehensible form (provided also that the victim has in that place a reputation which is thereby damaged).⁸⁶⁵ In opting for place of download as *locus delicti*, the court explained that in the case of online material, it does not become available in comprehensible form until downloaded onto the computer of someone who has used a web browser to pull the material from the web server.⁸⁶⁶ In other words, the downloading of the suspect material brings about the damage to reputation and it is the place of download that constitutes the *locus* for the commission of the tort of defamation.⁸⁶⁷

9.3.2 *Implications of the ruling*

The Dow Jones ruling is important for a number of reasons.

Firstly, the Australian High Court rejected the appellant's contention that the novel technological context of the internet called for a new and distinct concept of publication.⁸⁶⁸ Instead, the court made no allowances for the intrinsically global nature of the internet. It used the analogy of newspaper circulation and ruled that publication took place not in the place where the defamatory material was uploaded but rather where it was downloaded, i.e. in the place where the material was read and comprehended by publishees.

and the response (from the US) constituted one phenomenon and this was 'not a divisible operation'. He stated that the better view would appear to be 'that the information is published in both places at the same time. Not perhaps at the same time for a scientist counting in milliseconds but, for the law's purposes, no distinction can be sensibly drawn.' He went on to say that the message is as much published and delivered in Victoria as it is sent for delivery from New Jersey. *Gutnick v Dow Jones & Co Inc* [2001] VSC 305 [67]. In the judge's view, the information is released and received virtually instantaneously and the attempt to separate them for the law's purpose is a fallacy. *Ibid* [71]. Hedigan J went on to hold that the courts of the place of download (ie the State of Victoria) had jurisdiction to entertain the proceedings. *Ibid* [79].

⁸⁶⁴ *Dow Jones & Company Inc v Gutnick* [2002] HCA 56 [44].

⁸⁶⁵ *Ibid*.

⁸⁶⁶ *Ibid*.

⁸⁶⁷ *Ibid*.

⁸⁶⁸ *Ibid* [20].

In giving primacy to the place of download, the court focused on the effects of Dow Jones' conduct rather than the conduct itself. The effects of the appellant's conduct were injury to the respondent's reputation while the act of uploading in New Jersey constituted the appellant's conduct. By emphasising place of download, the court was following the approach adopted in cases of pre-internet media such as newspapers and TV. In such cases, the established place of the tort for the purposes of defamation is the place of 'publication', that is, the jurisdiction where the material was received or comprehended by a third party.

In the court's view, the substance of the action was the harm or the effects of the appellant's conduct. As the respondent's reputation was damaged in the state of Victoria where publishees downloaded and comprehended the defamatory material, the High Court had no difficulty finding that the Victorian courts were an appropriate forum.

Secondly, just like in *Berezovsky v Michaels*,⁸⁶⁹ the Australian High Court discounted the fact that only a tiny percentage of the subscribers to the relevant website were Australians.⁸⁷⁰ What was key was that a small but perfectly formed defamation had been committed in Australia, thereby permitting Victorian courts to assume jurisdiction.

9.3.3 Jurisprudential inconsistency, post-Dow Jones

While the *Dow Jones* ruling has, undoubtedly, a high profile, considerable jurisprudential inconsistency has emerged in this area in the common law world. For instance, a US Court of Appeals (4th Circuit) ruled in *Young v New Haven Advocate*⁸⁷¹ that Virginian courts did not have jurisdiction in a case of alleged online defamation despite the fact that the allegedly defamatory material⁸⁷² was accessible online in

⁸⁶⁹ *Berezovsky v Michaels* [2000] 1 WLR 1004.

⁸⁷⁰ Even the appellant was unsure as to how many Australians had a subscription to its website but on the basis of paid subscription fees linked to credit cards the holders of which gave Australian addresses, the appellant estimated that 1,700 of the subscribers to its website were Australians. Given that its website had 550,000 subscribers in total, the Australian component only constituted 0.30% of the total. *Dow Jones & Company Inc v Gutnick* [2002] HCA 56 [169].

⁸⁷¹ *Young v New Haven Advocate*, 315 F 3d 256 (4th Cir 2002).

⁸⁷² The defendant newspapers had published a story about the State of Connecticut's policy of housing prisoners in Virginian institutions and allegedly defamed the warden of a Virginian

Virginia and the plaintiff worked in that state. The defendants, two Connecticut newspapers - *The New Haven Advocate* and *The Hartford Courant* - invoked the doctrine of *forum non conveniens* against the plaintiff. The US Court of Appeals ruled that the Virginian courts did not have jurisdiction over the Connecticut-based newspapers because the newspapers did not ‘manifest an intent to aim their websites or the posted articles at a Virginian audience.’ The Court of Appeals followed its previous decisions which had stated that a plaintiff would need to prove that an out-of-state defendant’s internet activity was expressly targeted at, or directed to, the forum state in order to establish jurisdiction in the courts of that state. In this case, even though the plaintiff had allegedly suffered damage to his reputation in Virginia as a result of the articles, the evidence showed that the newspapers had intended to direct the publications at a (local) Connecticut audience,⁸⁷³ despite the article being accessible online in other jurisdictions.

9.3.4 English rulings which followed the Gutnick Approach

In contrast with the US, England adopted the *Gutnick* approach. This is evident from the rulings in *Harrods Ltd v Dow Jones Co Inc*⁸⁷⁴ and *Lewis v King*⁸⁷⁵. *Harrods* also involved allegations (by Harrods against Dow Jones) of online and offline defamation. The relevant article was published in the Wall Street Journal printed edition as well as on Dow Jones’ website which was accessed by a relatively small number of internet users in the UK. The article headed ‘The Enron of Britain’ referred to a possible floatation of Harrods. The plaintiff contended that the article imputed corporate untrustworthiness on its part and that if publicly listed, it would prove to be Britain’s Enron, defrauding and deceiving investors on a huge scale. Harrods commenced proceedings in England but Dow Jones invoked the doctrine of *forum non conveniens* in a bid to stay the proceedings. The court rejected Dow Jones’ inconvenient forum claim and held that an online article is deemed to be published where internet users downloaded, read and comprehended it. In addition, the High Court affirmed that the ‘single publication’ doctrine did not apply in English law.

prison (a Mr Young) by implying that he was a racist who encouraged the abuse of inmates by prison guards.

⁸⁷³ For the analogous ‘targeting members of the public’ in the context of the web-blocking cases, see paragraphs 6.10.2 and 6.10.3

⁸⁷⁴ *Harrods Ltd v Dow Jones Co Inc* [2003] EWHC 1162 (QB).

⁸⁷⁵ *Lewis v King* [2004] EWCA Civ 1329 [28]–[31].

Lewis v King involved litigation in the US between Don King the well-known boxing promoter and three defendants the best known of whom was Lennox Lewis (first defendant), the then British world heavy weight champion. In short, the proceedings represented Don King's libel claim for alleged internet publications by the third defendant, the lawyer representing Lewis in the American litigation. All of the parties were USA-based. King brought proceedings in the UK and was granted permission to serve out of the jurisdiction. The defendants sought to set that order aside.

The High Court held against the defendants. It ruled that it was an appropriate case for service outside of the jurisdiction as, applying the rule that publication takes place where material is heard or read and observing that the claim was limited to publications within England and Wales, the tort had been committed and the damage had been suffered within that jurisdiction. Secondly, the court deemed England and Wales the appropriate forum. The general presumption was that the appropriate forum was where the tort was committed. It was significant that the claimant had a substantial reputation within the jurisdiction, and that the relevant websites were popular and frequently accessed from within the jurisdiction.

On appeal, it was stated in the judgment that the parties accepted that a text on the internet is published at the place where it is downloaded.⁸⁷⁶

In opting for place of download only, the *Dow Jones*, *Harrods* and *Lewis* rulings are obviously more restrictive than the 'Reinwater'⁸⁷⁷ line of reasoning. However, *Dow Jones/Harrods/Lewis* deal specifically with an instance of *online* tort, in contrast with *Bier* which involves an offline tort.

Clearly, in terms of online libels, the place of download is the preminent locus for the purposes of localisation. *Bier* is somewhat out on a limb from a precedential value perspective. While it gives the claimant optionality in terms of the place to sue, its value is arguably diminished somewhat by the fact that it is an offline tort.

⁸⁷⁶ Ibid [2].

⁸⁷⁷ Case 21/76 *Handelskwekerij G J Bier BV v Mines de Potasse d'Alsace SA* [1976] ECR 1735 (analysed at para 4.2.3.2.) .

The key issue is how compelling are these various (defamation) rulings when it comes to an online *copyright* situation? The rationale in *Gutnick* seems to have established a firm foothold in the UK.

9.3.5 *The Defamation Act 2013*

In 2013, the UK adopted its Defamation Act. Section 8 of the Act introduces a single publication rule which replaces the multiple publication rule. The net effect of the single publication rule is that the limitation period in relation to any cause of action brought in respect of a subsequent publication is treated as having started to run on the date of the first publication. The rule also covers subsequent publications to a limited section of society, for example where a blog has a small group of subscribers or followers.⁸⁷⁸ Section 8(4) of the 2013 Act provides that the single publication rule does not apply where the manner of the subsequent publication (of the statement) is ‘materially different’ from the manner of the first publication. In determining this issue, courts may have regard to such things as: the level of prominence that a statement is given⁸⁷⁹ and, the extent of the subsequent publication.

9.3.6 *Two catalysts on the road to adoption of the Defamation Act 2013*

On the long road to adoption of the Defamation Act 2013, two catalysts are apparent. Firstly, in December 2002, the Law Commission published its preliminary investigation ‘Defamation and the Internet – A Preliminary Investigation’⁸⁸⁰ while, secondly, the Ministry of Justice published its consultation paper titled *Defamation and the internet: the multiple publication rule* on 16th September 2009.⁸⁸¹

⁸⁷⁸ Defamation Act 2013, s 8(2).

⁸⁷⁹ For example, a story may first appear relatively obscurely in a section of a website where several clicks are needed to access it. But, it is later transferred to the website’s homepage, where it receives a much higher number of hits.

⁸⁸⁰ Law Commission, *Defamation and the Internet – A Preliminary Investigation* (Scoping Study No 2, December 2002).

⁸⁸¹ Ministry of Justice, *Defamation and the internet: the multiple publication rule – Consultation Paper* (CP20/09, 16 September 2009).

9.3.6.1. The Law Commission's two Scoping Studies on Defamation and the Internet from 2002

Two scoping studies into aspects of defamation law and the internet were published by the Law Commission in 2002. The first concerned perceived abuses of the defamation procedure and was published in May 2002.

The second scoping study was published in December 2002 and highlighted four areas of concern: the liability of ISPs for other people's material; the application of the limitation period to online archives; the exposure of internet publishers to liability in other jurisdictions; and the risk of prosecution for contempt of court.

The Law Commission acknowledged that there were problems in the way in which the limitation period applied to online archives. Referring to the (then) 'standard English rule' (i.e. the multiple publication rule), the Law Commission stated that a cause of action accrues each time a libel is disseminated. As a consequence of this, the limitation period runs from each occasion on which a 'hit' is made on a website. Therefore, in terms of online archived newspapers, libel actions may be brought many years after their original publication, at which point it may be difficult for the publishers to mount an effective defence because records and witnesses are no longer available.⁸⁸² Clearly, this was an unsatisfactory situation. But so too was the claimant's situation as he was subject to a short one year limitation period.

Two principal reforms were suggested by the respondents who answered the Law Commission's questionnaire. The first was the adoption of the US single publication rule while the second was the provision of a specific archive defence for material that had been held for over a year.

In conclusion, the Law Commission stated that there was a need to review the way in which the multiple publication rule interacts with the limitation period applying to archived material. It felt that the one year limitation period might cause hardship to claimants due to insufficiency of time to prepare a case. Conversely, it felt it was also potentially unfair to defendants to allow actions to be brought against newspapers decades after their original publication, simply because copies had been placed in an

⁸⁸² Law Commission, *Defamation and the Internet – A Preliminary Investigation* (Scoping Study No 2, December 2002) paras 1.6 and 1.14.

archive. A lapse of time made it extremely difficult for a newspaper company to mount an effective defence as records and witnesses were no longer available. And both these disadvantages had to be set in the context of the social utility of online archives, as acknowledged by the Court of Appeal. The Law Commission recommended considering the issue further either through the adoption of a single publication rule or through a more specific defence that would apply to archives (whether online or offline).⁸⁸³

9.3.6.2. The Ministry of Justice's Consultation Paper

In its consultation paper 'Defamation and the Internet: the Multiple Publication Rule' and the response,⁸⁸⁴ published in March 2010, the Ministry of Justice reviewed the application of the multiple publication rule in the context of online content (especially archived content). The consultation paper solicited views on whether, in principle, the multiple publication rule should be retained and, if not, whether a single publication rule should be introduced. An alternative to a single publication rule is also mooted, i.e. amending the Defamation Act 1996 to extend the defence of qualified privilege to publications on online archives outside the one-year limitation period. Of the 34 responses received by the Ministry of Justice, 55 percent of the respondents favoured the introduction of a single publication rule.⁸⁸⁵

9.4. Conclusions

This chapter has revolved around the issue of pinpointing the *locus delicti* in the context of online defamation. Due to the relative lack of copyright-related jurisprudence, I relied on the analogue of online defamation as it involves an act of publication and therefore has parallels with the communication to the public right under UK copyright law.

In *Dow Jones v Gutnick*, the Australian High Court ruled that the tort of defamation was committed at the place of download. The rationale behind that approach was that place of download constitutes the place where the defamatory publication occurs as it was at that location that the defamatory material was read and comprehended by the publishee.

⁸⁸³ Ibid para 3.24.

⁸⁸⁴ Ministry of Justice, *Defamation and the internet: the multiple publication rule – Consultation Paper* (Response to consultation, CP(R) 20/09, 23 March 2010).

⁸⁸⁵ Patrick M Vollmer, *Defamation* (House of Lords Library Note, LLN 2010/016, 5 July 2010)

The natural follow on is that the defamed person's reputation is damaged at that time/in that place too.

In the same ruling, the court rejected the argument (by Dow Jones) that the location of the server was determinative. Instead, the Australian High Court focused on the place where the last event necessary to make the tortfeasor liable took place (i.e. place of download).

The English rulings of *Harrods v Dow Jones* and *Lewis v King* followed the general principle enunciated in *Gutnick*, thereby copper fastening the place of download as the pre-eminent locus for the purpose of localising online libels.

By including a single publication rule in its 2013 Defamation Act,⁸⁸⁶ the UK has followed the approach taken in the US. The rule will allow UK courts to deem an aggregate communication (publication, broadcast or transmission) a single publication. The Defamation Act also contains an interesting provision (section 9) on jurisdiction. It touches on the principle of *forum non conveniens* and refers to instances where the defendant is not domiciled in the UK or another EU Member State. In such circumstances, an English court may only assume jurisdiction in relation to multi-state torts if it is satisfied that of all the places in which the defamatory statement was published, England and Wales is 'clearly the most appropriate place in which to bring an action in respect of the statement'.

⁸⁸⁶ Defamation Act 2013, s 8.

Chapter 10. General Conclusions

Chapter 10.	303
10.1 Introduction: problems and solutions	304
10.2 PIL's slow adaptation to the online world	304
10.3 Dow Jones v Gutnick : place of upload or place of download?	305
10.4 Proxy war for the struggle between the single publication rule and the multiple publication rule?	306
10.5 Facilitative and non-facilitative elements (viewed from the perspective of Article 2, Brussels I)	308
10.5.1 Norwich Pharmacal relief (facilitative).....	309
10.5.2 Geolocation technology (facilitative).....	309
10.5.3 Data retention legislation (facilitative).....	311
10.5.4 The Dynamic Allocation of IP addresses (non-facilitative).....	312
10.5.5 Facilitative elements versus non-facilitative elements.....	312
10.6 Models and analogues for online copyright infringement	313
10.6.1 Reproduction right versus Defamation.....	313
10.7 Research Questions and Answers	316
10.7.1 Question 1.....	316
10.7.2 Question 2.....	317
10.7.3 Question 3.....	318
10.7.4 Question 4.....	318
10.7.5 How well established is the lex loci protectionis within Europe?.....	319
10.8 Some Final Conclusions	320

10.1 Introduction: problems and solutions

This thesis has exposed the very real and practical problems associated with applying the tort PIL rules to the internet. Superficially, some of the PIL rules appear to be susceptible to easy application but, when, transposed to an online environment, become considerably more difficult to apply. The fact that sovereign borders are not as clearly marked online as they are in the offline world does not assist the situation. *Dicey, Collins and Morris* puts it well when it states that:

it has not been easy for the conflict of laws to adapt itself to the changes in social and commercial life which the 20th century has witnessed. Many of its rules were laid down in the 19th century and seem better suited to 19th century conditions than to those of the 20th century.⁸⁸⁷

By logical extension, it would be even more difficult for the field of the conflict of laws to adapt itself to the 21st century, given that so many torts take place on the amorphous, border-disregarding internet nowadays. Pinpointing the *locus delicti* is always a challenge but this challenge is magnified many times in an online environment. The challenges involved in localising copyright's reproduction right, communication to the public right and the making available right in an online environment along with the analogue, online defamation, are critically evaluated in chapter 6 while an in-depth analysis of the landmark Australian cybertorts ruling - *Dow Jones v Gutnick*.⁸⁸⁸ occurs in chapter 9.

10.2 PIL's slow adaptation to the online world

In some ways, PIL is struggling to adapt to the online world. For a medium of communications that transcends sovereign borders it is perhaps unsurprising that it has a rather fraught relationship with a field of law so aligned with sovereign demarcations and discrete legal systems. But, the relationship between PIL and the internet seems an uneasy one, demonstrated by the two examples below, one with a global dimension, the other with an EU dimension.

⁸⁸⁷ Lord Collins of Mapesbury et al (eds), *Dicey, Collins and Morris: The Conflict of Laws*, Vol 1 (15th edn, Sweet & Maxwell 2012) 10.

⁸⁸⁸ *Dow Jones & Company Inc v Gutnick* [2002] HCA 56.

The first case relates to the proposed Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters which failed due to the proposers and draftsmen of that particular convention underestimating complexities created by the internet. This is ironic as the global and widespread use of the internet amplifies the need for an international instrument like the aforementioned.⁸⁸⁹ The second example points to the fact that the internet does not seem to feature prominently in the collective consciousness of EU legislators as evidenced by the fact that, of the three important PIL Regulations adopted in the EU since 2000 (Brussels I, Rome I and Rome II), only Rome I (through its Recital (24)) makes any reference to the internet and then, in only an oblique way.⁸⁹⁰

10.3 Dow Jones v Gutnick: place of upload or place of download?

Determining the *locus delicti* for an international online defamation was the key issue in the landmark Australian ruling in *Dow Jones v Gutnick*. There, the High Court of Australia was presented with two opposing points of view relating to alleged online defamation. Should an online publication be deemed to occur in the jurisdiction where the allegedly defamatory article was downloaded or, in the jurisdiction where it was uploaded? The publication, once comprehended by the publishee, caused damage to the victim's reputation ('the harmful event' in Brussels I parlance). In opting for place of download as *locus delicti*, the Australian High Court ensured that the State of Victoria would both assume jurisdiction of the case and have its laws applied in the proceedings. In terms of the push/pull dichotomy (examined in chapter 6), the publication and the attendant defamation only occurred after a 'pull' by the publishee. Viewed from a different perspective, the (defamatory) digital content hosted on the web server was only deemed published at the point of access, not at the point of storage.⁸⁹¹ It seems too, that in *Dow Jones*, the *locus delicti* was coterminous with the origin of the 'pull' (effected by the publishee).

⁸⁸⁹ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 288.

⁸⁹⁰ See para 1.6.

⁸⁹¹ At para 6.2.

10.4 Proxy war for the struggle between the single publication rule and the multiple publication rule?

In a slightly odd way, *Dow Jones* became the ‘arena’ for the struggle between two distinct rules of defamation. Invoking the single publication rule, Dow Jones argued that New Jersey should be deemed the place of publication as it was in that state that the defamatory article was placed on a server. Further, the appellant contended that Victoria was *forum non conveniens* as the laws of New Jersey should apply following its determinative act of placing the defamatory article on a server in that state.

Significantly, however, the single publication rule is not a legal doctrine followed in Australia. Instead, that country applies the multiple publication rule. In the High Court, the appellant argued that that court should reformulate Australian defamation law so as to incorporate the single publication rule and to designate the location of the server as the place of single publication.

Dow Jones further contended that the advent of the internet was a sufficiently revolutionary technological advancement so as to warrant a reconsideration of the law governing the elements of the tort of defamation.⁸⁹² As regards the place of wrong for choice of law purposes, Dow Jones argued that this should be ascertained by reference to where in substance the cause of action arose. In its view, the cause of action arose in either New Jersey or New York, both states being the location of its servers.

The High Court rejected the appellant’s view that jurisdiction be vested in the courts of the place of upload. This was done for a number of reasons. Firstly, the place of upload might bear little or no relationship to the place where the communication had its major impact. Secondly, publishers might manipulate the uploading of data so as to insulate themselves from liability in Australia or elsewhere. In other words, defamers could use a server in a jurisdiction in which the defamation laws are tilted decidedly towards defendants. Thirdly, the risk of an American legal hegemony was cited by Callinan J to reject the place of upload. Mr Justice Callinan’s viewpoint was coloured by the fact that back in 2002, a vastly disproportionate share of all internet servers in the world were located in the US. If place of upload were chosen as the determinative *locus* for determining jurisdiction, then that would, in Callinan J’s view, ‘confer upon one

⁸⁹² *Dow Jones & Company v Gutnick* [2002] HCA 56 [77] (Kirby J).

country ... an effective domain over the law of defamation'.⁸⁹³ Such a rule would, in the court's view, be to the financial advantage of publishers in the US and the serious disadvantage of those unfortunate enough to be reputationally damaged outside the US.⁸⁹⁴

By giving primacy to the place of download, the Australian High Court focused on the effects of Dow Jones' conduct rather than the conduct itself. The effects were injury to the respondent's reputation while the conduct was the act of uploading to servers in New Jersey. Somewhat ironically, and despite the case being one of the most significant cybertorts rulings ever, Australia's highest court followed the approach in cases concerning pre-internet media such as newspapers and TV, by attaching greatest importance to place of publication. This in effect, was the jurisdiction where the defamatory material was received or comprehended by the publishee (the place of download). While this approach is defensible in cases of defamation (where a publication is necessary), it cannot be carried across uncritically to copyright.

Not all online torts are subject to the place of download rule. Pertinently, two online IP infringement rulings examined earlier in this thesis support the place of upload approach. They are the Cristal case (*Castellblanch SA v Champagne Louis Roederer SA* [2004] IL Pr 41)⁸⁹⁵ concerning online trademark infringement, and the Scottish ruling *Alan MacKie t/a 197 Aerial Photography v Nicola Askew, Largsholidaylets.co.uk*.⁸⁹⁶ In chapter 6, considerably more complex localisation rules are in evidence in relation to the communication to the public right and the making available right.

⁸⁹³ Ibid [200] (Callinan J).

⁸⁹⁴ See Chp 9, para 9.3.1. It is arguable that Callinan J's comments are equally applicable to copyright as the statistics for 2013 show that the US is preeminent in terms of the number of servers on its territory. However, the analysis as to locus of infringement (for copyright) takes its own course (see chapter 6 and Appendix 2 generally). As regards statistics on location of servers/hosting of websites, see: Superb Internet, 'Study: Where the Web is located and Ghost Servers Haunting the Internet' (24 May 2013) <<http://www.superb.net/blog/2013/05/24/study-where-the-web-is-located-ghost-servers-haunting-the-internet/>> accessed 10 June 2014.

⁸⁹⁵ See para 9.3.1., footnote 838 .

⁸⁹⁶ *Alan MacKie t/a 197 Aerial Photography v Nicola Askew, Largsholidaylets.co.uk* [2009] SLT (Sh Ct) 146.

10.5 Facilitative and non-facilitative elements (viewed from the perspective of Article 2, Brussels I)

In the intermeshing analysis carried out in chapters 7 and 8, this thesis examined elements that are deemed facilitative or non-facilitative of the operation of Article 2, Brussels I and the related crucial task of identifying the tortfeasor.

In short, three facilitative elements were identified while two non-facilitative elements were identified. However, as regards the non-facilitative elements, only dynamic allocation of IP addresses was discussed in detail (though anonymising software/techniques are recognised as a non-facilitative element).

The facilitative elements are: *Norwich Pharmacal* relief, geolocation technology and data retention legislation (dealt with in chapter 7). The non-facilitative elements are dealt with in chapter 8.

Of the three facilitative elements critically evaluated, all offer support in terms of tortfeasor identification but two of the elements have become slightly weakened by jurisprudential developments in recent times. They are: the data retention component, affected by the recent CJEU ruling in *Digital Rights Ireland*⁸⁹⁷ and *Norwich Pharmacal* relief which may well be restricted following the rulings in *Media C.A.T.*⁸⁹⁸ and *Smith v ADVFN*.⁸⁹⁹ It is arguable that the strongest facilitative element is the geolocation technology element,⁹⁰⁰ the only technological element of the three. This technology enables the linking of IP addresses to physical locations, thereby offering the possibility of defendant identification. However, even geolocation technology has some chinks in its armour. I shall now draw some conclusions on the three facilitative elements and the non-facilitative element.

⁸⁹⁷ The ruling is analysed from para 7.4.4. onwards.

⁸⁹⁸ See para 7.3.2.7.

⁸⁹⁹ See para 7.3.2.6.

⁹⁰⁰ See para 7.5.

10.5.1 Norwich Pharmacal relief (facilitative)

From the perspective of actually identifying a tortfeasor, *Norwich Pharmacal* relief is still, without doubt, facilitative. Particularly so, when one considers that the DEA 2010 is, for all intents and purposes, in abeyance.⁹⁰¹ While the web-blocking rulings under section 97A of the CDPA 1988⁹⁰² prevent infringing activities by blocking illegal websites, they do not produce the names and addresses of individual copyright infringers, as occurs under a NPO.⁹⁰³

Two recent rulings – *Smith v ADVFN* and, *Media C.A.T.*⁹⁰⁴ possibly portend a more critical and cautious approach by UK courts to this form of equitable relief. Following *Smith v ADVFN*, it seems that the courts will carefully consider whether the material complained of is, in fact, defamatory. In addition, *Norwich Pharmacal* relief will only be available if the claimant cannot obtain the relevant document(s) from another source or by other means.

Media C.A.T. too represents a more critical interpretation Judge Birss, perceiving certain weaknesses in the *Norwich Pharmacal* system, drew inspiration from the system of *Anton Piller* orders, to suggest the appointment of a neutral supervising solicitor to ensure that the NPO and any information disclosed under it were not abused. *Media C.A.T.* may yet act as a catalyst for a complete reappraisal of the *Norwich Pharmacal* jurisdiction. Possible reforms that might flow from such reappraisal include greater restrictions being placed on information disclosed under NPOs along with court directions on the use of the information disclosed.

10.5.2 Geolocation technology (facilitative)

Svantesson's comment on geolocation technology, discussed in chapter 7, is probably one of the most compelling in relation to this particular technology. He stated that

⁹⁰¹ The key provision of the DEA 2010 that could assist rightholders in identifying copyright infringers – Section 4 (obligation on ISPs to provide infringement lists to copyright owners) – is currently not in operation.

⁹⁰² See para 7.3.5.

⁹⁰³ There are parallels between *Norwich Pharmacal* relief and the Enforcement Directive (2004/48/EC). Art 8(1) of the latter refers specifically to proceedings concerning an infringement of an IPR and empowers the competent judicial authorities to order that information relevant to the infringement be made available to a claimant upon his request.

⁹⁰⁴ Analysed at paras 7.3.2.6 and 7.3.2.7. respectively.

geolocation technologies should not be seen as an alternative to using PIL to erect protective borders on the internet. Rather the application of PIL must recognise the value of geolocation technologies and non-technical geolocation for the identification of geographical location.⁹⁰⁵

This form of pragmatic thinking will, likely, chart a way forward for PIL in the online world. A symbiotic relationship between the field of law (PIL) and the facilitative technology (geolocation technology) is an important first step in smoothing the application of PIL to copyright infringements on the internet.

With its capability of identifying geographical location on the internet, geolocation technology undoubtedly offers tangible help to both the courts and lawyers. It was deployed as an evidential tool in the *Yahoo!* and *Gutnick* cases while it was acknowledged and endorsed in two US rulings - *National Federation of the Blind v Target Corporation*, and *Hageseth v Superior Court*, and one German ruling - *VGH Bayern*, 10 CS 08.2399.⁹⁰⁶

No doubt, geolocation service providers will continue to improve the accuracy of their geolocation technology and improving accuracy will persuade courts to attach even greater importance to these technologies, thereby creating a virtuous circle. While there is not absolute consensus on the effect IPv6 will have on the accuracy of geolocation, both Olsen and Jacobus contend that the expanding IP address system will have a significantly positive impact on the accuracy of geolocation technology.⁹⁰⁷ Olsen even argues that IPv6 would make the identification of the physical location of an internet user a rather trivial task.

As geolocation technology is gradually transforming the internet into a medium that takes account of geographical and legal borders, it would be short-sighted of lawyers and the courts to ignore the potential benefits offered by this technology.

Despite the many benefits that flow from geolocation technology, its use is not problem-free. Doubts remain about the accuracy levels of the technology and there have

⁹⁰⁵ At para. 7.3.16.

⁹⁰⁶ At para 7.3.14

⁹⁰⁷ At para 7.3.14.

been statements from such quarters as the Article 29 Data Protection Working Party, the Information Commissioner's Office (Good Practice Note titled 'Collecting Personal Information Using Websites') and Germany's former data protection commissioner, Peter Schaar that IP addresses should be viewed as personal data. This could place quite serious legal and commercial strictures on geolocation service providers.

On balance, however, geolocation technology constitutes a fillip for both the courts and copyright owners, a fillip that is likely to grow rather than diminish with the passage of time.

10.5.3 Data retention legislation (facilitative)

Despite the recent CJEU holding in *Digital Rights Ireland* that the Data Retention Directive is invalid,⁹⁰⁸ it has to be borne in mind that in the UK, the transposing legislation – the Data Retention (EC Directive) Regulations 2009 (SI 2009/859) – is still in force and may not be automatically invalid.⁹⁰⁹ Like all legislation, the 2009 Regulations could be affected by function or scope creep, whereby data retained for one purpose – law enforcement – could also be used for other purposes. Lobbying by the CMBA has already occurred,⁹¹⁰ whereby that association (representing the digital content industry) had demanded that access to retained data should also be granted for the purpose of investigating other crimes such as IP infringement. This could lead to a situation where an instrument brought in as an anti-terrorism measure may, in the future, be used to prosecute file-sharers.

It is almost inevitable that a period of legal uncertainty will follow the CJEU ruling. There is now a strong likelihood that national transposing measures will be challenged in all of the Member States, meaning that the 2009 Regulations may meet the same fate as the legal instrument that inspired their adoption. As the declaration of invalidity by the CJEU takes effect from the date on which the directive entered into force, this element of retrospection could still seriously impact the outcome of court rulings long since concluded, where the evidence relied on was data retained under the directive.

At EU level, it is hard to see a replacement directive being adopted in early course. In the meantime, the Luxembourg ruling may further galvanise those in Europe who have

⁹⁰⁸ For an analysis of this ruling, see para 7.4.4.

⁹⁰⁹ At para 7.4.

⁹¹⁰ At para 7.4.3.

been campaigning for a Digital Bill of Rights which would enshrine the right of privacy for netizens.

At bottom, the *Digital Rights Ireland* ruling represents a privacy victory that makes subsequent drafting of data retention rules challenging as the European Commission will have to acknowledge the strength of the fundamental rights enshrined in Articles 7 and 8 of the Charter of Fundamental Rights of the EU and ensure that they are adequately provided for in any new law.

10.5.4 The Dynamic Allocation of IP addresses (non-facilitative)

This non-facilitative element is treated in chapter 8 of the thesis. When it comes to the dynamic allocation of IP addresses, *BMG Canada v John Doe* and *EMI Records (Ireland) Limited v Data Protection Commissioner* demonstrate how IP addresses are not assigned to the MAC addresses sequentially. Accordingly, IP addresses are not associated with any one account holder nor are they allocated in any predetermined pattern. As a consequence, it is not possible to directly identify an account holder merely from an IP address.

Evidence adduced in *BMG Canada v John Doe* by BMG Canada's employees revealed that the task of linking a name and address of an account holder to a specific IP address is far from straightforward and would involve cross-referencing the IP address to a database of MAC addresses and then cross-referencing the MAC address with the account database. To compound problems, the more historic the search, the less reliable the information. Clearly, the process of linking an IP address with a real person (possibly defendant) is neither straightforward nor fast. And, from an evidential perspective, much would hinge on how carefully the cross-referencing between the various sets of data is carried out.

10.5.5 Facilitative elements versus non-facilitative elements

On the basis of the four elements examined in this thesis (across chapters 7 and 8), it is clear that the application of the PIL tort rules to the internet will not be entirely straightforward. It goes without saying that black letter law cannot provide solutions for something like the dynamic allocation of IP addresses but it does seem that through a 'coalition' of the three facilitative elements (*Norwich Pharmacal* relief, geolocation technology and data retention laws), the application of key jurisdictional provision such

as Article 2, Brussels I, will be made easier. Put differently, the black letter law alone may be inadequate and, for it to work efficaciously, it will be dependent on a ‘coalition’ of equitable relief, technology and data retention provisions/principles to provide the necessary evidence for locus to be determined.

10.6 Models and analogues for online copyright infringement

Chapter 6 was given over to critically evaluating and comparing the two online torts which form the backbone of this doctoral research, namely, online copyright infringement (the case study) and, the analogue - online defamation. The aim was to determine how compelling (or not) the defamation analogue actually is. I also highlighted what I felt were points of connection (crossover points) and points of disconnection between the various torts. In terms of the making available right, I critically evaluated localisation criteria formulated by Sterling and, separately, by the European Commission.⁹¹¹

From this point on, I shall specify by heading which 2 torts are being compared in terms of conclusions.

10.6.1 Reproduction right versus Defamation

My findings are that there are more points of disconnection than points of connection between these two torts and that online defamation does not read so easily onto online infringement of the reproduction right. Rather, the approach taken by Svantesson can be developed and applied to the analysis of copyright infringement. The principal point of connection between the two torts exists at the level of the ISP where, by virtue of the E-Commerce Directive, the ISP could avail of exemptions under Articles 12 (mere conduit) and 14 (hosting) for both defamatory material and content which infringes the reproduction right in copyright.

⁹¹¹ Severine Dusollier et al, ‘Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society’ (*European Commission*, 2013)

<http://ec.europa.eu/internal_market/copyright/docs/studies/131216_study_en.pdf>
accessed 5 May 2014.

One significant disconnect between these 2 torts is the delayed harmful event in the case of defamation. As defamation requires the publishee to comprehend the defamatory material before the injury arises, there is therefore a (necessary) third party involvement which can slow down the commission of the tort and have a negative knock on effect for the cause of action.

This potentially delayed cause of action contrasts with an online copyright infringement where the cause of action arises the instant the protected material is infringed. In sum, the infringement of the reproduction right potentially becomes actionable at a much earlier stage than defamation. Analysed differently, online copyright infringement cases do not require the 'intervention' of a third party for the cause of action to accrue.

The possibility of immediate actionability in respect of an online copyright infringement is a very real benefit as torrent tracking sites (which have increased in number recently) assist rightholders to discover quite quickly if their copyright material has been infringed.

10.6.2 Online Communication to the public versus online defamation

One significant point of disconnection between the localisation of online communication to the public and online defamation is the requirement that there be a targeting of the public in the former. In the cases based on Section 97A CDPA 1988 (analysed from para 7.3.5. onwards), it was this targeting of a UK public that localised the tort in the UK, thereby justifying assumption of jurisdiction by the UK courts.

Another point of disconnection between the torts is the verifiability of the factors that go to make up the tort. When applying the 'targeting the public' test, the English High Court uses predominantly commercial and social/cultural factors, such as: language; advertising and origin of the internet traffic. As these factors are readily verifiable, a decision on localisation can be taken speedily. In contrast, when it comes to online defamation, the commission of the tort often occurs in a private setting. The tort takes place when the publishee downloads (and comprehends) the defamatory material. But, this will often involve a discrete and private act by the publishee, something considerably less verifiable than the factors outlined for targeting the public. Put

differently, localising an act of online defamation is more difficult to achieve than localising an online communication to the public, primarily because the factors to be verified in the latter are more public and therefore more ascertainable.

10.6.3 Localisation of the making available right

There is commonality between Sterling and the European Commission⁹¹² in terms of possibly localising the making available right at the place where the server (upon which the works are hosted) is located. However, the European Commission also expresses some scepticism about this criterion as it acknowledges possible difficulties in determining the actual location of the servers.

These difficulties could be exacerbated if the infringing material is spread over different servers in different countries. While Sterling considers the two classic broadcasting theories – the communications theory and the emission theory – in the context of localising the making available right, he ultimately rejects the emission theory as he does not believe it to be practicable in an online setting.⁹¹³ Factors that make the emission theory unworkable according to Sterling are: the absence of an identifiable transmission point⁹¹⁴ and the risk of the infringing material being stored on multiple servers. In endorsing the communications theory, Sterling implicitly accepts that the making available takes place at the point of reception. In contrast with Sterling, the European Commission makes no reference to either of the broadcasting theories in its study.

Applying the communications theory may not be entirely problem-free. There may be many points of reception for the digital material, making the localisation quite challenging. It is also interesting to note the CJEU's ruling in *Football Dataco v*

⁹¹² The views of the European Commission are set out in its previously mentioned 'Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society'.

⁹¹³ There is an interesting parallel between Sterling's viewpoint and the view of the CJEU in rejecting the Emission Theory in Case C-173/11 *Football Dataco v Sportradar* [2013] CMLR 29, analysed at para. 3.6.4.5.

⁹¹⁴ In justifying its rejection of the Emission Theory in *Football Dataco v Sportradar*, the CJEU also adverted to the risk of localising the originating server, see para 3.6.4.5.

Sportradar where that court seemed to keep all its options open by remaining open to both the emission and communications theory.⁹¹⁵

10.7 Research Questions and Answers

Having set out my general conclusions, I shall now recapitulate my original research questions and provide answers to same.

10.7.1 Question 1

What are the main practical difficulties that arise in terms of applying the EU tort PIL rules to the internet?

The two principal difficulties are linked to Articles 2 and 5(3), Brussels I. The former relates to identification of the defendant (IP infringer) while the latter relates to localisation of the IP infringement ('the harmful event' in the parlance of Brussels I)

As regards the difficulty linked to Article 2, where the claimant fails to identify an online infringer (defendant), the possible action comes to nought. A potentially worse scenario might unfold were the IP owner to misidentify the infringer. In such a situation, the IP owner could leave himself exposed to an action in defamation. A misidentification of infringer is not as far-fetched as it may sound. After all, the accuracy of geolocation technology is still impugned in some quarters and, an ISP may commit an error when attempting to comply with a NPO.

In cases of IP infringement, it is very difficult to say where the act of infringement occurred when there is a whole sequence of events between the original uploading (input) of information and its eventual display on a screen. This situation is compounded if the infringement traverses a number of countries. However, even in this complicated sequence of events, there will always be two really significant events (or, constants) – the uploading of the information and its eventual downloading.

In cases of online IP infringement, if there is a failure to pinpoint the *locus delicti*, there will be negative consequences for the claimant IP holder though, as the option to sue in the country where the harm (tort) occurred would then disappear, thereby forcing him to sue the defendant in the latter's place of domicile (under Article 2, Brussels I).

⁹¹⁵ Para 3.6.4.6.

However, this might not necessarily be the claimant's preferred forum in which to litigate.

10.7.2 Question 2

What role does technology play in conflicts scenarios in the twenty-first century? And, on balance, who derives greater benefit from technology - the claimant (IP owner) or the defendant (IP infringer)?

Technology plays an important and growing role in PIL situations. In chapter 7, I referred to the growing prominence of geolocation technology in court proceedings and even in legislation.⁹¹⁶

Currently, client-side geolocation technologies offer the highest degree of accuracy, deploying as they do, a user-centric model. Such technologies operate using GPS and wireless tower triangulation and frequently, iPhones and GPS-equipped wireless devices can be located within a radius of a few dozen feet which is as close as you will get to precise geographic location. Naturally, from a PIL perspective, this is a significantly better situation than server-side geolocation tools which can only locate most users within a twenty to thirty mile radius.⁹¹⁷

On balance, the IP owner benefits more as geolocation technology continues to improve in terms of accuracy and it has been endorsed by the courts in the US and continental Europe.⁹¹⁸ There is a good prospect that this technology will become well-established as an evidential tool in the court system. As anonymity on the internet/anonymising software do not come within the scope of this thesis, they have not been considered in depth. That said, however, the author recognises the real risk posed by anonymising software when it comes to digital copyright/rightsholders' interests on the internet.

⁹¹⁶ See para 7.3.13.

⁹¹⁷ As to accuracy levels of geolocation technology in general, see para 7.3.12

⁹¹⁸ At para 7.3.14

10.7.3 Question 3

In terms of applying Articles 2 and 5(3), Brussels I, to an internet environment, which elements are either facilitative or non-facilitative when it comes to the effective application of those provisions?

The facilitative elements comprise *Norwich Pharmacal* relief, geolocation technology and data retention legislation. A non-facilitative element is the leasing or dynamic allocation of IP addresses (but there is acknowledgement that anonymising software/techniques also constitute a non-facilitative element, but they were not covered in this thesis)

10.7.4 Question 4

In terms of applying Article 5 (3), Brussels I, to online IP infringements, how useful is the analogue of online defamation?

At para 6.9.2. of this thesis, I set out the points of disconnection between online infringement of the reproduction right and online defamation. The principal disconnection is the ‘delayed’ harmful event in online defamation, often caused by the publishee only comprehending the defamatory material quite some time after it was originally sent. But, this also results in a delay in terms of the cause of action accruing to the victim.

This potentially delayed cause of action contrasts with an online copyright infringement where the cause of action arises the instant the protected material is infringed. In other words, the online copyright infringement becomes actionable at an earlier stage (potentially, much earlier stage) than the online defamation, for infringement of reproduction and communication rights

In addition, in copyright infringement cases, there is no requirement that there be third party involvement (i.e. the publishee). Infringement of copyright material occurs once the act of primary infringement occurs – there is no requirement that a recipient takes possession of the infringing material. The commission of the tort in an online IPR scenario is more immediate than in an online defamation scenario.

One could argue that the immediate actionability of the online copyright infringement is more theoretical than real, *but*, with the growing number of torrent tracking sites, this increases the likelihood of infringing copies being discovered soon after their creation. Interestingly, a 2012 study conducted by Birmingham University indicates that an illegal file-sharer downloading popular content would be logged by a monitoring firm within three hours.⁹¹⁹

10.7.5 How well established is the lex loci protectionis within Europe?

Clearly, Article 8(1), Rome II, makes provision for the *lex loci protectionis* in situations where copyright is infringed. The rule is further bolstered by Recital (26) of the same Regulation. However, the suggestion in that provision that the *lex loci protectionis* is ‘a universally acknowledged principle’ is perhaps going a bit too far as, even before the adoption of Rome II, there was no consistent practice among the Member States.

The *lex loci protectionis* is found in a number of national laws to include the Belgian Code of Private International Law, the Swiss Private International Law Act 1987, the Italian Private International Law Act 1995 and the German partial codification of tort and property choice of law rules.

Curiously, while the Austrian Private International Law Act 1978 provides for the *lex loci delicti*, that country’s Supreme Court and a number of authors have effectively interpreted it to mean the *lex loci protectionis*.

While there is not a universal preference for the *lex loci protectionis*, there seems to be a clear tendency towards various slightly different *lex loci protectionis* approaches. A country which does not apply the *lex loci protectionis* is the Netherlands. Instead, it applies the *lex loci delicti* by virtue of its 2001 Private International Law Act on Torts which has no specific rule on Intellectual Property.

10.8 Some final conclusions

One key benefit derived from using and adapting Svantesson’s defamation model was that it enabled me to extend my analysis in terms of online tort localisation to two other of copyright’s restricted rights, namely the communication to the public right and the making available right. In terms of my research on the communication to the public

⁹¹⁹ See para 6.9.2.

right, that led me to the webblocking cases and the ‘targeting the public test’, applied by the English High to determine if an infringing communication to the public could be localised in the UK. In critically evaluating the localisation of the making available right, I could draw on the findings of both Sterling and the European Commission.

The localisation ‘template’ that I used in chapter 6 allowed me to position the findings conveniently so that I could also draw on pertinent EU legislation (e.g. the E-Commerce Directive) that might influence an issue like liability when it comes to an ISP’s ‘involvement’ in an online tort.

In systematically separating actions and harms in the defamation/reproduction part of the ‘template’, it is entirely feasible for this part of the model to be applied to other online torts in the future so as to determine *locus delicti*.

As regards the making available right, Dusollier’s criterion No 3 (Where the material act of upload is initiated)⁹²⁰ represents an attempt to return to the unitary-right model first used by the Cable and Satellite Directive, whereby the location of a broadcast for copyright/licensing purposes was identified as the single State of uplink. Some commentators predicted that the Cable and Satellite Directive would be overtaken by digitisation,⁹²¹ meaning that rights would follow the InfoSoc Directive, which, arguably reflects a traditional territorial approach. However, my research (at paras 6.10 to 6.10.3) shows that by adopting a ‘targeted push’ model of online communication to the public, the web-blocking cases have avoided the most fragmented version of the purely territorial approach that would flow from following *Dow Jones v Gutnick*. Instead, these cases have put online communication to the public on a jurisdictional footing similar to cable and satellite, in a way which is compatible with the ‘new public’ approach of *FAPL v QC Leisure (analysed at 3.6.1.)*.

⁹²⁰ At para 6.18

⁹²¹ For instance, Bernt Hugenholtz, see: , 'Copyright without Frontiers: is there a future for the Satellite and Cable Directive' (*IViR*, 2005)
<<http://www.ivir.nl/publications/hugenholtz/copyrightwithoutfrontiers.pdf>> accessed 13 June 2014

Appendix 1 (Literature Review)

LIST OF PRINCIPAL WORKS CONSULTED

Objective of this Appendix

Literature Review

1. Kono – Intellectual Property and Private International Law – Comparative Perspectives (2012)
2. Svantesson – Private International Law and the Internet (2012)
3. Fawcett and Torremans – Intellectual Property and Private International Law (2011)
4. Leible and Ohly – Intellectual Property and Private International Law (2009)
5. Dickinson – The Rome II Regulation – The Law Applicable to Non-Contractual Obligations (2008)
6. Gottschalk et al – Conflict of Laws in a Globalised World (2007)
7. Drexler and Kur - Intellectual Property and Private International Law (IIC Studies - Studies in Industrial Property and Copyright Law) (2005)
8. Basedow et al (eds) - Intellectual Property in the Conflict of Laws (2005)
9. Mireille van Eechoud – Choice of Law in Copyright and Related Rights. Alternatives to the Lex Protectionis (2003)

Objective of this Appendix

This Appendix is a literature review of the principal works published over the last ten years or so which are relevant to my doctoral thesis, to include textbooks, monographs and edited volumes. Interestingly, quite a number of the works reviewed are based on conferences/symposia, proving that the delicate interface between IP and PIL is being discussed and debated at public fora more and more. Examples of the last-mentioned category include the works by Leible and Ohly, Basedow, Drexl, Kur and Metzger and, lastly, that by Drexl and Kur.

One thing that this appendix highlights is the growing importance and profile of the complex interface between IP and PIL. This is evidenced by a growing number of exemplary specialist textbooks on this interface with Continental European authors very prominent in this regard.

Literature Review

The subject-matter of the vast majority of the works referred to in this appendix is *directly* relevant to my thesis. Admittedly, Svantesson's work is *somewhat* of an odd man out, given its strong consumer contracts and defamation focus. However, the tortious character of the last-mentioned element of course ensures the relevance of Svantesson's book to this PhD, as does the incorporation of the treatment of trade marks in the second edition (2012) of the work. The fact that the work looks at the thorny interface between PIL and the internet is already ample justification for its treatment in this doctoral dissertation. The analogue of online defamation, treatment of online trade marks infringement and the all-important analysis of geo-identification and geolocation technologies (in chapter 10) ensure, together, that Svantesson's work comes within the scope of analysis of my PhD.

I now propose treating the principal relevant textbooks to this thesis in reverse chronological order, commencing with the very recently published *Intellectual Property and Private International Law, Comparative Perspectives*, by Kono (ed).

Kono – Intellectual Property and Private International Law – Comparative Perspectives (2012)⁹²²

This work grew out of the 18th International Congress of Comparative Law and comprises the General and National Reports arising from said congress. It offers a comparative law perspective on a range of core issues covering more than twenty countries across North America, Europe (EU Member States and third countries) and Asia. The topics covered are diverse and include: issues of personal and subject-matter jurisdiction, provisional and protective measures, the law applicable to the creation and transfer of IPRs and their infringement, problems raised by parallel and concurrent proceedings and the recognition/enforcement of foreign judgments. In addition, the following are all considered: the CLIP proposals, the ALI proposals, the reform of the Brussels I Regulation and the potential impact of the Hague Choice of Court Convention. Kono's book does not omit developments in Asia. The Transparency of Japanese Law Project (analogous to the ALI and CLIP Principles) and the Korean Waseda project are covered. The Waseda group, established by scholars in Waseda University has, as its objective, the drafting of a proposal on jurisdiction and applicable law for the whole East Asian region. Running parallel with the aforementioned proposal is a separate proposal for the revision of domestic Korean PIL in order to make the cross-border adjudication of IP disputes more effective. Ultimately, the intention is to unify both sets of Principles.

Svantesson – Private International Law and the Internet (2012)

A textbook which marries two of this thesis' core elements - PIL and the internet, is that written by Dan Jerker B Svantesson and published in 2012 (2nd edn) entitled simply but appositely, *Private International Law and the Internet*.⁹²³ The book's relevance derives from the following facts: 1. One of its primary foci is online defamation (which, like IP infringement, is tortious in nature); 2. A treatment of trade marks is included in the current edition; and 3. An entire chapter (Chapter 10) is devoted to geolocation (or geo-identification) technologies. Besides these two elements, the book very helpfully examines the internet's core characteristics.⁹²⁴ Early in this chapter, Svantesson states

⁹²² Toshiyuki Kono (ed), *Intellectual Property and Private International Law – Comparative Perspectives* (Hart Publishing 2012).

⁹²³ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012).

⁹²⁴ In chapter 2, titled 'Approaching the Internet'.

that ‘internet communications challenge traditional models of regulation and governance’.⁹²⁵ In effect, it is a unique combination of features that makes internet communication significantly different. This combination comprises the following characteristics: the borderlessness of the internet (the internet is sometimes described as border-disregarding); the internet’s geographical independence (it is very easy to make internet communication available to people across geographical borders);⁹²⁶ the lack of geographical indicators (particularly as regards domain names and e-mail addresses)⁹²⁷ and the lack of central control of the internet/internet communications.⁹²⁸

Tellingly, Svantesson observes that the internet’s unique set of characteristics have profound implications for jurisdictional issues. Refusing to pull any punches, he states that ‘certain rules of PIL have *lost* their logical bases’.⁹²⁹ Concluding that particular chapter of his book, Svantesson states presciently:

Finally, the observation that internet communications are associated with a unique set of characteristics allows us to draw one last, fundamental and for the rest of this book decisive conclusion – the application of existing conflict of laws rules to internet-fact scenarios cannot be described as the mere application of old rules or principles. Instead, it must be acknowledged that, due to the social, economical and technical peculiarities of internet technology, any such application, in fact, constitutes an expansion of the scope of the pre-existing rule or principle.⁹³⁰

⁹²⁵ Dan Jerker B Svantesson, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012) 29.

⁹²⁶ This characteristic is manifested in two ways: For the one imparting information, it is easy to make internet communication available to people across geographical borders. For the ones seeking information, the geographical location of that information is virtually irrelevant in most forms of internet communication. Another aspect of internet communication being geographically independent is that it is virtually instantaneous. For instance, the time difference between visiting a local website (i.e. stored on a local server) and visiting a geographically distant website is minimal. *Ibid* 35 et seq.

⁹²⁷ However, when it comes to IP addresses, Svantesson qualifies his assessment somewhat. This is due to the emergence of ‘increasingly accurate so-called geo-location technologies’. These technologies represent the technical means for connecting an IP address with a physical location. Svantesson alludes to the increasing use of mobile devices, such as PDAs, smart phones and tablets and the related need to consider additional mechanisms for geographical identification such as Global Positioning System (GPS). *Ibid* 44 et seq.

⁹²⁸ In its very structure and architecture, the internet is decentralised. Svantesson makes the interesting observation that PIL rules too have never operated in a climate where a single international authority sets the regulatory standard. *Ibid* 49 et seq.

⁹²⁹ *Ibid* 61 (emphasis added).

⁹³⁰ *Ibid* 62.

One of the very real advantages of the latest edition of *Intellectual Property and Private International Law* is that it treats the online aspects of the IP/PIL interface in much greater detail than did the first edition (published in 1998). In fact, two chapters of the second edition are given over to internet-related issues, namely, chapters 10 and 17. The former, titled ‘Infringement, the Internet and Broadcasting: Jurisdiction’ encompasses such elements as: characteristics of the internet, infringement over the internet, sale of infringing goods over the internet, complementary torts committed over the internet (one of which is defamation) and lastly, broadcasting. The latter, titled ‘Choice of Law and the Internet’ commences by specifying the real clash taking place between the global or ubiquitous nature of the internet and the territorial approach, which is the founding principle of the IP universe. It then analyses the difficulties in determining place of reproduction in alleged online copyright infringement cases. (Does it occur when content is pulled up onto the user’s screen or must the content be saved by the user onto his PC hard drive before reproduction occurs?) It then distinguishes between these localisation issues and PIL issues in the strict sense. In reality, the choice of law process and the choice of law rules are unaffected. Rome II Regulation, Article 8 applies and it is up to the claimant to determine for which countries he seeks protection.

Importantly, Chapter 17 examines the instance of ubiquitous infringement (facilitated by ubiquitous media, such as the internet). As the term suggests, these cases are truly global ones where infringement *potentially* happens in every single country. In effect, we are probably really only talking about internet- and satellite-related IP breaches here as they are the only media with truly global reach. Tellingly, the authors imply that the preponderant example of ubiquitous IP infringement is online copyright infringement:

What is necessarily ubiquitous are the means of communication used to commit the infringement. The potentially global case can only happen if, say, the internet is used. Then means of communication must be ubiquitous. In practice, we are concerned with copyright infringement on the internet.⁹³²

⁹³¹ James J Fawcett and Paul Torremans, *Intellectual Property and Private International Law* (2nd edn, OUP 2011).

⁹³² *Ibid* 918.

In instances of ubiquitous infringement, it would be unfair if the infringer who posted the infringing document could, on the basis of *insignificant* use, see a large number of different laws potentially applied against him, each time in respect of minuscule damage. Instead, what is justifiable is the application of a single law to the case, most probably the law with the closest connection to the infringement. Both, the European Max Planck Group for Conflict of Laws in Intellectual Property (CLIP) and American Law Institute (ALI) proposals, have ubiquitous infringement provisions.⁹³³ However, the two proposals differ somewhat in the criteria (factors) they use to determine which State has the closest connection with the infringement.⁹³⁴

Leible and Ohly – Intellectual Property and Private International Law (2009)⁹³⁵

An edited work – *Intellectual Property and Private International Law* by Stefan Leible and Ansgar Ohly, was published in 2009. The book is based on a Bayreuth conference (4/5 April 2008) of the same name and comprises papers presented at that conference. From the perspective of this thesis, the most relevant papers are the following:

1. Annette Kur's 'Are there any common European principles of Private International Law with regard to Intellectual Property?'
2. Axel Metzger's 'Jurisdiction in Cases Concerning Intellectual Property Infringements on the Internet – Brussels I Regulation, ALI principles and Max Planck Proposals' in Stefan Leible and Ansgar Ohly (eds), *Intellectual Property and Private International Law* (1st edn, Mohr Siebeck 2009) 251 – 267
3. Frank Beckstein's summary of the presentation given by Rochelle Dreyfuss titled 'The American Law Institute Project on Intellectual Property: Principles Governing Jurisdiction, Choice of Law and Judgments in Transnational Disputes'

⁹³³ The CLIP provision is Article 3:603: Ubiquitous Infringement, while the relevant ALI principle is Section 321: Law or Laws to be applied in cases of ubiquitous infringement.

⁹³⁴ The relevant factors in the CLIP rule are: (a) the infringer's habitual residence; (b) the infringer's principal place of business; (c) the place where substantial activities in furthering of the infringement in its entirety have been carried out; and, (d) the place where the harm caused by the infringement is substantial in relation to the infringement in its entirety. As regards the ALI Principles, the relevant factors are as follows: (a) where the parties reside; (b) where the parties' relationship, if any, is centred; (c) the extent of the activities and the investment of the parties; and, (d), the principal markets towards which the parties directed their activities.

⁹³⁵ Stefan Leible and Ansgar Ohly (eds), *Intellectual Property and Private International Law* (1st edn, Mohr Siebeck 2009).

The first paper, by Annette Kur, titled ‘Are there any common European principles of Private International Law with regard to Intellectual Property?’ is quite self-explanatory. Kur’s paper also explores whether the so-called common European principles are distinguishable from those which apply outside Europe, particularly, the US. The scope of Kur’s paper covers the CLIP project (Max Planck Institutes in Munich and Hamburg) and some of the characteristic features of the counterpart US project - the ALI Principles.

As regards the applicable law in relation to non-contractual obligations, Kur makes some interesting observations. She states that even before the Rome II Regulation was adopted, the PIL principles applying in Europe with regard to IP infringements were common in that the *lex loci protectionis* prevailed in respect of approximately 95% of pre-Rome II law and practice in EU Member States. Kur also contends that by virtue of Rome II, Article 8(1), a somewhat modified version of Berne Convention, Article 5(2) will become part of European black letter law. In the words of Kur, this incorporation of Article 5(2) into the European applicable law legal framework ‘lends a different accent to long-standing debates about the character of the *lex protectionis* as a choice of law rule derived from international norms such as national treatment or Berne Convention, Article 5(2) itself’.⁹³⁶

Kur makes an interesting observation about infringements perpetrated through ubiquitous media such as the internet. In such cases, the infringement arguably occurs in every country that is reached by the communication. In such cases, the courts may derogate from the *lex protectionis* by applying the law which is most closely connected with the infringement in its entirety. She acknowledges that such a principle could, under certain circumstances, unduly favour the interests of the plaintiff (typically the right holder). In cases of ubiquitous infringement, the plaintiff may have an opportunity to bring world-wide proceedings in her home country. Further, he may then additionally profit from the natural tendency of courts to assume that the law having the closest connection to a case is the law of the forum.

To maintain a balance however, the aforementioned principle has a counterweight (rule) whereby any party may prove that the law applying in a country/countries covered by

⁹³⁶ Annette Kur, ‘Are there any common European principles of Private International Law with regard to Intellectual Property?’ in Stefan Leible and Ansgar Ohly (eds), *Intellectual Property and Private International Law* (1st edn, Mohr Siebeck 2009).

the dispute differs, in aspects which are essential for the decision, from the law identified by the court as the law having the closest connection. In such a case, the court shall apply the different laws unless this leads to inconsistent judgments, in which case the differences are taken into account in fashioning the remedy.

Metzger starts his article ‘Jurisdiction in Cases Concerning Intellectual Property Infringements on the Internet – Brussels I Regulation, ALI principles and Max Planck Proposals’ by referring to the trend of consolidation in terms of jurisdictional issues and offers as the clearest landmark of this consolidation process, the final approval of the American Law Institute of the ‘Intellectual Property Principles Governing Jurisdiction, Choice of Law and Judgments in Transnational Disputes’ in May 2007. Reference is then made to an important European academic project initiated by the Max Planck Institute (Munich) which published draft principles on jurisdiction in intellectual property cases in 2004. Lastly, Metzger describes a follow-up project commenced in 2004 by the Max Planck Institutes in Munich and Hamburg as an international project with members from six Member States of the EU and the US. Titled the ‘European Max Planck Group for Conflict of Laws in Intellectual Property (CLIP)’, the objective of the project was to formulate a comprehensive set of principles on jurisdiction, applicable law, recognition and enforcement.

In this short analysis of Metzger’s paper, I shall focus on special jurisdiction (*forum delicti*), in essence, the framework of Brussels I, Article 5(3).

Metzger makes an important observation about the *locus delicti* under Article 5(3) when he states that ‘the ECJ has not yet decided on the interpretation of the provision in internet cases’.⁹³⁷

Looking at the duality of jurisdictional options under *Bier*,⁹³⁸ Metzger posits two possible places upon which jurisdiction could be based - firstly, place of download and secondly, place where the defendant mainly acted or at the place of the server of the website. Either, Metzger argues, could constitute the place where the event giving rise to the damage took place. As regards basing jurisdiction on place of download, Metzger

⁹³⁷ Axel Metzger, ‘Jurisdiction in Cases Concerning Intellectual Property Infringements on the Internet – Brussels I Regulation, ALI principles and Max Planck Proposals’ in Stefan Leible and Ansgar Ohly (eds), *Intellectual Property and Private International Law* (1st edn, Mohr Siebeck 2009) 255.

⁹³⁸ *Handelskwekerij G J Bier BV v Mines de Potasse d’Alsace SA* [1976] ECR 1735 (the ‘Reinwater’ case).

cites a number of Continental European judgments which support this position, e.g. *Roederer* (French Cour de Cassation)⁹³⁹ and ‘Red Bull’ (Austrian Oberster Gerichtshof).⁹⁴⁰ However, this approach has lost much of its influence of late as it is overly wide and creates many problems for defendants. For instance, IP infringers who use peer-to-peer or YouTube to disseminate/display infringing material could end up being sued anywhere in the world where the infringing material is downloaded. A possible solution comes by limiting jurisdiction to those countries where the alleged infringement has commercial effect⁹⁴¹ or substantial impact compared to the infringement as a whole. The second option - granting jurisdiction to the courts of the place where the acts of the alleged infringer occur – ties in with Article 2:202 of the Final Text of CLIP’s Principles on Conflict of Laws in Intellectual Property (2011) which provides that the infringer must have acted in the relevant State (to initiate or further the infringement) or must have directed activity to that State before the courts of such State can assume jurisdiction.

Metzger contends that localising the place of activity may cause practical problems in internet cases. Given the ease of manipulation of the server, the location of the server is not an adequate determination. Metzger finally localises the place of activity at the place where the upload of internet services were initiated or controlled.⁹⁴²

In disputes concerned with infringement of an intellectual property right, a person may be sued in the courts of the State where the alleged infringement occurs or may occur, unless the alleged infringer has not acted in that State to initiate or further the infringement and his/her activity cannot reasonably be seen as having been directed to that State.

⁹³⁹ *Castellblanch SA v Champagne Louis Roederer SA* [2004] IL Pr 41, [2004] Rev Crit DIP 632.

⁹⁴⁰ OGH 24.4.2001, GRUR Int 2002, 265 (‘Red Bull’ case).

⁹⁴¹ The commercial effect concept has already found international consensus on a substantive law level in the WIPO, ‘Joint Recommendation Concerning Provisions on the Protection of Marks, and other Industrial Property Rights in Signs, on the Internet’ (845(E), 24 September - 3 October 2001) <<http://www.wipo.int/export/sites/www/freepublications/en/marks/845/pub845.pdf>> accessed 9 May 2014.

⁹⁴² Axel Metzger, ‘Jurisdiction in Cases Concerning Intellectual Property Infringements on the Internet – Brussels I Regulation, ALI principles and Max Planck Proposals’ in Stefan Leible and Ansgar Ohly (eds), *Intellectual Property and Private International Law* (1st edn, Mohr Siebeck 2009) citing James J Fawcett and Paul Torremans, *Intellectual Property in Private International Law* (1st edn, OUP 1998) 143.

Another elucidating piece in the Leible/Ohly work is that by Frank Beckstein. Beckstein analyses the presentation given by Rochelle Dreyfuss on the American Law Institute's project on Intellectual Property and Conflicts, to include jurisdiction, choice of law and recognition/enforcement elements. The final draft of these Principles received approval by the membership of the ALI on 14 May 2007 and, at the time of Beckstein's writing, the final text of the Principles was going to be published imminently.

Professor Dreyfuss explained that the point of origin of the ALI project was the suspension of the work on the Draft Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters of the Hague Conference of PIL. The objective of the Principles is to serve the courts as guidelines. Courts can rely on these Principles, wherever applicable, as long as their use is not against the law of the forum.

The scope of the Principles, settled in Section 102, is deemed to be very broad, applying as they do to both registered and unregistered IPRs. An important limitation of the scope of the Principles is the requirement of transnational civil dispute.

The ALI Principles distinguish between personal and subject matter jurisdiction. As regards personal jurisdiction, the Principles at Section 204 offer three different options. First, an alleged infringer of IP may be sued in any State in which that person has substantially acted (Section 204(1)). A court at the place of the substantial act can deal with all injuries that arise from that activity. A second basis for jurisdiction is the place where the activities are directed. In such case, however, the competence of the court in the relevant State will be limited to injuries that arise in that specific location (Section 204(2)). The third basis relates to infringement havens. As WTO membership is viewed as a kind of 'proxy' of good law, non-WTO countries are viewed as potential infringement havens. Other important requirements are that the defendant solicits or maintains contact, business or an audience in the non-WTO country on a regular basis (Section 204(3)). In short, under this jurisdictional basis, if infringers distribute infringing (US) copyright-protected material from non-WTO States, then US courts are competent with respect to the full geographic scope of the harm, if the infringer directs its activities to the US and has enough contacts or business there.

The Principles differentiate between personal and subject matter jurisdiction and a court can only entertain a suit if it has power both over the litigants and the subject matter. Jurisdiction over the subject matter depends on the powers given by the respective State

and the court cannot exceed its legislatively defined competence over the issues by reference to the Principles (Section 211(1)).

The Principles also suggest rules for the execution of the rules on subject matter jurisdiction (Sections 211(2) – 214). As special focus is placed on local law, the parties are obliged to present their case, wherever possible, under local law, and, consistent with the scope of personal jurisdiction under these Principles, with all transactionally related claims in a single court. The courts shall extend their subject matter to all claims and counter claims arising from the initial activity (Section 212). However, the parties are not obliged to bring all claims in the same court and can present their cases in different courts. Under the ALI Principles, therefore, the violation of various patents in the same invention can be adjudicated in one forum, unlike the situation that prevailed under the Federal Circuit's decision in *Voda v Cordis*.⁹⁴³

On the issue of the applicable law, Prof Dreyfuss stated how the ALI had adopted the *lex loci protectionis* as a general principle for the major issues, i.e. the existence, validity, duration, attributes, infringement and remedies (Section 301). In terms of defining the *lex loci protectionis*, it is the law of the State of registration for registered rights and, for unregistered rights, it is the law of the place where protection is sought, ie where the infringing act has or will have an impact.

A special rule for ubiquitous infringements is also contained in the ALI Principles (Section 321). It is similar to the ideas in the CLIP project as both groups cooperated in that matter. Thus, in cases where infringement is ubiquitous, the Principles allow for the issues of existence, validity, duration, attributes, infringement and remedies to be governed by the law with the closest connection to the entire case (rather than a multiplicity of laws). It is also possible to simplify the dispute by applying not one single law, but instead a small number of laws that are closely connected to the case.

In conclusion, Professor Dreyfuss considered the value and the practical relevance of the ALI Principles. She believes that the project will promote further discussion and greater effort to resolve the problems arising from transnational disputes in IP. It may also shift the focus from efforts to over-harmonise IP laws to investigating ways to make global litigation less costly and time-consuming. On a distinct issue, as IP disputes become increasingly global, Prof Dreyfuss and her fellow reporters believe that

⁹⁴³ *Voda v Cordis*, 476 F 3d 887 (Fed Cir 2007).

atomised approaches by single countries cannot be the answer in the long run. Alternatives to the atomised approach, such as the extraterritorial application of IP law and the creation of a system of unitary rights worldwide are unlikely to be acceptable or, come into force. Because of the shortcomings of alternative approaches, Prof Dreyfuss advocates a system of efficient litigation of the national IPRs as set out in the ALI Principles.

Dickinson – The Rome II Regulation – The Law Applicable to Non-Contractual Obligations (2008)

In 2008, a specialist text on the Rome II Regulation was published by Andrew Dickinson.⁹⁴⁴ As Rome II features prominently in this thesis, the relevance of the work goes without saying. It is also fitting that a book came out so promptly after the regulation's adoption as the instrument clearly constitutes a landmark in PIL. The regulation's importance derives from the fact that it is both the first EU instrument of general application harmonising rules of applicable law and the most comprehensive instrument of its kind anywhere in the world.⁹⁴⁵ Chapter 8 of Dickinson's work proved particularly relevant as it treats Intellectual Property. The analysis of Rome II, Article 8(1) (which governs the applicable law in the context of non-contractual obligations arising from an infringement of an IPR) is dealt with in chapter 5 of this thesis.

Gottschalk et al – Conflict of Laws in a Globalised World (2007)

A 2007 work which commemorates the pioneering work of Professor Arthur Taylor von Mehren (Harvard Law School), *Conflict of Laws in a Globalised World*,⁹⁴⁶ has two principal foci. Firstly, transatlantic litigation and judicial cooperation in civil and commercial matters, and secondly, choice of law in transatlantic relationships. In terms of the former, Christian Thiele's chapter 'The Hague Convention on Choice-of-Court Agreements: Was it Worth the Effort?' carries relevance for this PhD. In terms of the latter, Eckart Gottschalk's chapter titled 'The Law Applicable to Intellectual Property Rights: Is the Lex Loci Protectionis a Pertinent Choice-of-Law Approach?' also

⁹⁴⁴ Andrew Dickinson, *The Rome II Regulation – The Law Applicable to Non-Contractual Obligations*, *Oxford Private International Law Series* (OUP 2008).

⁹⁴⁵ Ibid Preface.

⁹⁴⁶ Eckart Gottschalk et al (eds), *Conflict of Laws in a Globalised World* (1st edn, CUP 2007). This work is, in fact, a commemoration of the works of Professor Arthur von Mehren (Harvard Law School) who had developed new thinking in the fields of private international law and comparative law and who passed away in 2006, having spent 50 years teaching law.

contains many components which fall within the scope of this thesis. Some of the core elements in Gottschalk's chapter are the following: the tensions that exist between the *lex loci protectionis*⁹⁴⁷ and the *lex originis*;⁹⁴⁸ how the *lex loci protectionis* has been explicitly codified in many of the recent codifications of PIL;⁹⁴⁹ whether the national treatment clause in Berne Convention, Article 5(2), points towards the law of the protecting country or is simply a non-discrimination rule?; What is the scope of the *lex loci protectionis*? Does it only cover the extent of protection, or does it also include the creation of copyright including questions of initial ownership?; Recent codification projects to encompass the *then* Discussion Draft produced by the American Law Institute titled 'Intellectual Property: Principles Governing Jurisdiction, Choice of Law and Judgments in Transnational Disputes' (finalised and published in 2008)⁹⁵⁰ and the *then* draft Rome II Regulation (with focus on Article 8(1)); and, finally, the challenges posed when the *lex loci protectionis* is applied in the context of multi-State conflicts.⁹⁵¹

Drexl and Kur - Intellectual Property and Private International Law (IIC Studies - Studies in Industrial Property and Copyright Law) (2005)

This work is a collection of symposium papers put together in the guise of *Intellectual Property and Private International Law – Heading for the Future (IIC Studies)*.⁹⁵² The relevant symposium, held in July 2003, was 'Jurisdiction and Choice of Law in

⁹⁴⁷ Under this choice-of-law rule, IPRs are governed by the law of the State for whose territory protection is claimed.

⁹⁴⁸ Under this choice-of-law rule, IPRs are governed by the law of the country from which they originate.

⁹⁴⁹ For example, Swiss Private International Law Act (1987), art 110(1), which served as a model for later codifications throughout Europe - for Belgium: Code of Private International Law (2004), art 93(1); for Italy: Law No 218/1995, art 54(1); for the Republic of Korea: Private International Law Act, revised by Law No 6465/2001, Section 24; for Austria: the doctrine and the Supreme Court have interpreted the Private International Law Act 1978, as amended, art 34(1) as referring to the law of the State for which protection is claimed.

⁹⁵⁰ Analysis revolves around Section 301 ('Territoriality') which deals with the applicable law in cases of IP infringement (i.e. for registered rights, the law of each State of registration and, 'for other intellectual property rights', the law of each State for which protection is claimed) and Section 321 ('Ubiquitous Infringements'). Sub-section (1) of Section 321 permits the parties and the court to agree to apply the law(s) of the State(s) with the closest connection to the dispute 'in exceptional cases'.

⁹⁵¹ Two principal challenges manifest themselves. Firstly, the courts have to deal with a multitude of legal systems and, as a corollary, a mosaic of applicable laws. Secondly, the forum courts may be inclined to apply the *lex loci protectionis* extraterritorially, which tends to result in overregulation.

⁹⁵² Josef Drexl and Annette Kur (eds), *Intellectual Property and Private International Law – Heading for the Future (IIC Studies)* (Hart Publishing 2005).

Intellectual Property Matters - Perspectives for the Future (Europe and Worldwide)'.⁹⁵³ It marked the culmination of a project concerned with the elaboration of draft provisions on jurisdiction and enforcement of foreign judgments in IP matters that had been conducted at the Max Planck Institute since spring 2001.

From the perspective of this thesis, the most relevant papers in this collection of symposium papers are: Andrea Schulz's piece, 'The Hague Conference Project for a Global Convention on Jurisdiction, Recognition and Enforcement in Civil and Commercial Matters: An Update', Richard Fentiman's 'Choice of Law and Intellectual Property', 'The Proposed Rome II Regulation: European Choice of Law in the Field of Intellectual Property' by Josef Drexler and, lastly, Ansgar Ohly's 'Choice of Law in the Digital Environment'.

While Ohly's chapter acknowledges that the *lex loci protectionis* prevails in IP disputes,⁹⁵⁴ he also observes that conflicts and infringements of IPRs on the internet make a fresh analysis of the traditional approach to the choice of law in IP disputes inevitable.

Ohly singles out three initiatives that exemplify this fresh analysis. The first initiative commenced in 1998 when the WIPO Standing Committee on the Law of Trademarks, Industrial Designs and Geographical Indications elaborated principles concerning the use of marks and other distinctive signs on the internet. After several rounds of discussions, the Joint Recommendation Concerning Provisions on the Protection of Marks and Other Industrial Property Rights in Signs on the Internet was adopted at a joint session of the Paris Union and the WIPO General Assembly in 2001.

The second initiative took the form of a draft international agreement on jurisdictional matters in the area of IP Law. This draft agreement, which was put together by Rochelle Dreyfuss and Jane Ginsburg, was later adopted as a project by the American Law Institute. The ALI broadened the parameters of the project to include choice of law and judgment components in transnational disputes. Those additional elements survived and featured in the final set of Principles which were published by the ALI in 2008.⁹⁵⁵

⁹⁵³ This symposium was organised by the Max Planck Institute for Intellectual Property, Competition and Tax Law.

⁹⁵⁴ Referring to the Swiss Act on Private International Law, art 110(1) in the process.

⁹⁵⁵ American Law Institute, 'Intellectual Property: Principles Governing Jurisdiction, Choice of Law and Judgments in Transnational Disputes' (WIPO, 2008) <<http://www.wipo.int/wipolex/en/details.jsp?id=7687>> accessed 13 July 2012.

The Working Group on Questions of Jurisdiction and Choice of Law in Intellectual Property Matters,⁹⁵⁶ initiated by the Max Planck Institute for Intellectual Property, Competition and Tax Law (Munich), constitutes the third initiative. This Working Group actually draws on the expertise found in the last-mentioned Institute and the Max Planck Institute for Comparative and Private International Law (Hamburg). Together, these institutes organised a joint conference ‘Intellectual Property in the Conflict of Laws’ in March 2004 at which representatives of the European Commission, the ALI, and the Hague Conference reported on the current status of legislative efforts and legal projects.⁹⁵⁷

Basedow et al (eds) - Intellectual Property in the Conflict of Laws (2005)

The book, *Intellectual Property in the Conflict of Laws*⁹⁵⁸ comprises papers given at the Hamburg Symposium held on the 2 and 3 March 2004. The symposium was organised by two of the leading centres of study in the fields of law concerned, namely, the Max Planck Institute for Comparative and Private International Law (Hamburg) and the Max Planck Institute for Intellectual Property, Competition and Tax Law (Munich).⁹⁵⁹ In terms of relevance to this thesis, one paper from the Hamburg symposium stands out, namely, Graeme Dinwoodie’s ‘Conflicts and International Copyright Litigation: The Role of International Norms’. In short, the most compelling points from Dinwoodie’s paper are as follows: The tendency of US and EU courts to increasingly permit the adjudication of claims under foreign copyright law⁹⁶⁰; the fact that he is open to the suggestion that Article 5(2), Berne Convention may not constitute a choice of law rule; that author’s acknowledgement of the growing harmonisation of copyright laws into what could ultimately be a ‘supranational copyright code’ (as suggested by Ginsburg);⁹⁶¹

⁹⁵⁶ Max Planck Institute for Comparative and International Private Law Hamburg, ‘Working Group on Questions of Jurisdiction and Choice of Law in Intellectual Property Matters’ (8 June 2010) <http://www.mpipriv.de/ww/en/pub/research/research_work/international_private_law_proc/commercial_and_competition_law/workgroup_intellectual_propert.cfm> accessed 13 July 2012.

⁹⁵⁷ A volume containing the conference papers was published at the start of 2005: Jürgen Basedow et al (eds), *Intellectual Property in the Conflict of Laws* (Mohr Siebeck 2005).

⁹⁵⁸ Ibid.

⁹⁵⁹ Stig Stromholm, ‘Preface’ in Jürgen Basedow et al (eds), *Intellectual Property in the Conflict of Laws* (Mohr Siebeck 2005).

⁹⁶⁰ For example, *Boosey & Hawkes Music Pubs v The Walt Disney Co*, 145 F 3d 481 (2nd Cir 1998).

⁹⁶¹ Jane C Ginsburg, ‘International Copyright: From a “Bundle” of National Copyright Laws to a Supranational Code’ (2000) 47 J Copyright Soc’y USA 265 (as referred to in Graeme B Dinwoodie, ‘Conflicts and International Copyright Litigation: The Role of International

his analysis of how in the US, courts and scholars have sought different ways to apply a single law to a multinational dispute and, finally, the various devices used by the US to extrude US law globally e.g. the exercise of jurisdiction over foreign acts where there exists a ‘predicate act’ in the US that facilitates copyright infringement abroad.⁹⁶²

Mireille van Eechoud – Choice of Law in Copyright and Related Rights. Alternatives to the Lex Protectionis (2003)⁹⁶³

The central objective of this work is to determine which conflict rules are suitable for contemporary copyright and related rights. Van Eechoud attempts to answer that central question from the viewpoint of the aims of choice-of-law and of the policies that underlie substantive copyright and related rights law.

In van Eechoud’s work, there is an acknowledgement that the advent of the Information Society has laid bare the shortcomings of the traditional territorial approach to copyright and related rights.⁹⁶⁴ This acknowledgement provokes a natural follow-on question: whether conflict rules based on a territorial view of IP are (or possibly ever were) adequate? And, if not, what changes should be recommended?

Van Eechoud also makes the point that while a number of authors interpret Article 5(2), Berne Convention as espousing the *lex protectionis*,⁹⁶⁵ this is not a unanimous

Norms’ in Jürgen Basedow et al (eds), *Intellectual Property in the Conflict of Laws* (Mohr Siebeck 2005).

⁹⁶² Dinwoodie lists the following rulings as examples of this jurisdictional policy: *Los Angeles News Serv v Reuters TV Int’l Ltd*, 149 F 3d 987 (9th Cir 1998) (unauthorised transmission and copy of work made in the US and then further transmitted to Europe and Africa); *Update Art, Inc v Modiin Publishing, Ltd*, 843 F 2d 67, 72-73 (2d Cir 1988) (unauthorised copy of plaintiff’s poster made in the US and then further copied and distributed in Israel); and *Sheldon v Metro-Goldwyn Pictures Corp*, 106 F 2d 45 (2d Cir 1939) (awarding plaintiff profits from both US and Canadian exhibition of infringing motion picture where a copy of the motion picture had been made in the US and then shipped to Canada for exhibition).

⁹⁶³ Mireille van Eechoud, *Choice of Law in Copyright and Related Rights. Alternatives to the Lex Protectionis (Information Law Series)* (Kluwer Law International 2003). Mireille van Eechoud, ‘Choice of Law in Copyright and Related Rights. Alternatives to the Lex Protectionis’ (DPhil thesis, University of Amsterdam 2003).

⁹⁶⁴ Mireille van Eechoud, *Choice of Law in Copyright and Related Rights – Alternatives to the Lex Protectionis* (Kluwer Law International 2003) 5.

⁹⁶⁵ Mireille van Eechoud, ‘Choice of Law in Copyright and Related Rights. Alternatives to the Lex Protectionis’ (DPhil thesis, University of Amsterdam 2003) 107, fn 302. Van Eechoud lists the following authors: Cruquenaire, Hoeren and Quaadvlieg, to name but a few. Alexandre Cruquenaire, ‘La Loi applicable au droit d’auteur: état de la question et perspectives’ (2000) 3 *Auteurs & Media* 210, 211; Thomas Hoeren, ‘IPR und EDV–recht. Kollisionrechtliche Anknüpfungen bei internationalen EDV-Verträgen’ (1993) 3 *CR* 129, 131; AA Quaadvlieg, ‘Een multiple personality syndrome in het IPR: de identificatie van de

viewpoint. Viewing the history of Article 5(2) and the difficulties that arise when it is regarded as a conflicts rule, van Eechoud's argues that it should not be considered as reflecting the *lex protectionis* or any other conflict rule, for that matter.⁹⁶⁶

auteursrechthebbende' in SCJJ Kortmann et al, *Op recht: bundel opstellen, aangeboden aan prof. mr. A.V.M. Struycken ter gelegenheid van zijn zilveren ambtsjubileum aan de Katholieke Universiteit Nijmegen* (WEJ Tjeenk Willink 1996) 255, 260.

⁹⁶⁶ Mireille van Eechoud, 'Choice of Law in Copyright and Related Rights. Alternatives to the Lex Protectionis' (DPhil thesis, University of Amsterdam 2003) 109.

Appendix 2 - Referring to Chapter 6 - Analytical Steps (Dusollier 2 does not fit into table)

Tort/infringement [‘NO’, ‘YES’ indicate whether committed at this point in space &time]	Defamation, online	Copyright – Reproduction online	Copyright - Communication by making available, online, on demand
Step 1 compose/copy & save	Compose defamatory material & save on own computer NO	Copy protected material and save on own computer YES, unless permitted act	Keep protected material on own computer NO
Step 2 Dispatch	Send/ upload NO	Upload NO (not by sender, at least)	Sterling 1 Dusollier 3 YES Upload to P2P website in EMI YES, if targeted EMI, FAPL vBSkyB. And if new public? Dramatico
Step 3 Transmission and intermediary storage	Storage on server NO	3a repro in course of transmission to server YES subject ‘mere conduit’ 3b storage on server YES 3c repro in transmission to recipient, as 3a	Sterling 2 (server) YES Dusollier 1 (server) NO
Step 4 recipient takes possession	Receives email, accesses web site but does not read/ comprehend NO	Storage, ie Repro in recipient’s computer, device YES (primary liability on	Download YES Sterling 3 No Dramatico

		<i>recipient</i>) subject to local authorisation /permitted acts	
Step 5 recipient reads/ listens/ watches	and comprehends content tending to H,R,C: YES <i>Dow Jones v Gutnick</i>	Repro on recipient's computer YES subject to temporary repro defence	As for broadcasting?
Step 5 Immediate harm	Immediate damage to reputation (hatred, ridicule, contempt) YES	No further infringement; goes to damages	No further infringement; goes to damages
Step 6 Consequential harm	Goes to damages if not too remote	Goes to damages if not too remote	Goes to damages if not too remote
	Defamation	Copyright repro	Copyright comm by making available

BIBLIOGRAPHY

UK LEGISLATION

Acts:

Anti-Terrorism, Crime and Security Act 2001 (c 24)

Broadcasting Act 1990 (c 42)

Communications Act 2003 (c 21)

Copyright, Designs and Patents Act 1988 (c 48)

Data Protection Act 1998 (c 29)

Defamation Act 2013 (c 26)

Digital Economy Act 2010 (c 24)

Limitation Act 1980 (c 58)

Obscene Publications Act 1959 (c 66, Regnal 7 and 8 Eliz 2)

Patents Act 1977 (c 37)

Private International Law (Miscellaneous Provisions) Act 1995 (c 42)

Regulation of Investigatory Powers Act 2000 (c 23)

Trade Marks Act 1994 (c 26)

Unfair Contract Terms Act 1977 (c 50)

Statutory Instruments:

Civil Procedure Rules 1998, SI 1998/3132 (L 17)

Rules of the Supreme Court (RSC), now The Civil Procedure (Amendment) Rules 2000,
SI 2000/221 (L 1)

The Civil Jurisdiction and Judgments Order 2001, SI 2001/3929

The Civil Jurisdiction and Judgments Regulations 2007, SI 2007/1655

The Copyright and Rights in Databases Regulations 1997, SI 1997/3032

The Retention of Communications Data (Code of Practice) Order 2003, SI 2003/3175

The Retention of Communications Data (Extension of Initial Period) Order 2003,
SI 2003/3173

The Retention of Communications Data (Further Extension of Initial Period) Order 2005,
SI 2005/3335

The Data Retention (EC Directive) Regulations 2007, SI 2007/2199

The Data Retention (EC Directive) Regulations 2009, SI 2009/859

The Intellectual Property (Enforcements, etc) Regulations 2006, SI 2006/1028

Draft legislation:

The Copyright and Rights in Performances (Disability) Regulations 2014

The Copyright and Rights in Performances (Personal Copies for Private Use) Regulations 2014

The Copyright and Rights in Performances (Quotation and Parody) Regulations 2014

The Copyright and Rights in Performances (Research, Education, Libraries and Archives) Regulations 2014

The Copyright (Public Administration) Regulations 2014

UK CASES

ABCI (Formerly Arab Business Consortium International Finance and Investment Co) v Banque Franco Tunisienne [2003] 2 Lloyd's Rep 146 (CA)

ABKCO Music & Records Inc v Music Collection International Ltd [1995] RPC 657

Alan MacKie t/a 197 Aerial Photography v Nicola Askew, Largsholidaylets.co.uk [2009] SLT (Sh Ct) 146

Alfred Dunhill Ltd v Diffusion Internationale de Maroquinerie de Prestige [2002] IL Pr 13

Ashton Investments Ltd v OJSC Russian Aluminium (Rusal) [2006] EWHC 2545 (Comm)

Ashworth Hospital Authority v MGN Ltd [2002] 1 WLR 2033; [2002] 4 All ER 193

Berezovsky v Michaels [2000] 1 WLR 1004

Bonnier Media Ltd v Smith; sub nom Bonnier Media Ltd v Kestrel Trading Corp [2002] SCLR 977

Boys v Chaplin [1971] AC 356

British South Africa Co v Companhia de Moçambique [1893] AC 602

Coca Cola Company v British Telecommunications plc [1999] FSR 518

Def Lepp Music v Stuart-Brown [1986] RPC 273

Dolphin Maritime & Aviation Services Ltd v Sveriges Angfartygs Assurans Forening
[2009] 2 Lloyd's Rep 123

Domicrest v Swiss Bank [1999] QB 548

Dramatico Entertainment Limited v British Sky Broadcasting Limited [2012] EWHC
1152 (Ch)

Dramatico Entertainment Limited v British Sky Broadcasting Limited [2012] EWHC
268 (Ch)

Drummond-Jackson v British Medical Association [1970] 1 All ER 1094

Duck v Bates [1884] 13 QBD 843

Duke of Brunswick v Harmer [1850] 3 Car & K 10

Duke of Brunswick v Harmer [1849] 14 QB 185

EMI Records (Ireland) Limited & Ors v The Data Protection Commissioner & Anor
[2012] IEHC 264

EMI Records Limited v British Sky Broadcasting Limited [2013] EWHC 379 (Ch)

Fort Dodge Animal Health Ltd v Akzo Nobel NV [1998] FSR 222

Francis Day & Hunter v Bron [1963] 1 Ch 587

Golden Eye (International) Ltd v Telefonica UK Ltd [2012] EWCA Civ 1740

Golden Eye (International) Ltd v Telefonica UK Ltd [2012] EWHC 723 (Ch), [2012] RPC 28

Grant v Google UK Ltd [2005] EWHC 3444 (Ch)

Grovit v De Nederlandsche Bank [2007] EWCA Civ 953

Harding v Wealands [2006] UKHL 32

Harms (Incorporated) Ltd v Martans Club Ltd [1927] 1 Ch 526

Harrods Ltd v Dow Jones Co Inc [2003] EWHC 1162 (QB)

Henderson v Jaouen [2002] EWCA Civ 75; [2001] 1 WLR 2971 (CA)

Hesperides Hotels Ltd v Muftizade [1979] AC 508

House of Spring Gardens Ltd v Waite (No 2) [1991] 1 QB 241

Jonathan Cape Ltd v Consolidated Press Ltd [1954] 1 WLR 1313

Judith Vidal-Hall and others v Google Inc [2014] EWHC 13 (QB)

Kitechnology BV v Unicor GmbH Plastmaschinen [1994] IL Pr 568

Lewis v King [2004] EWCA Civ 1329

Loutchansky v Times Newspapers Ltd (No 2) [2001] EWCA Civ 1805; [2002] 1 All ER 652

Lucasfilm Ltd v Ainsworth [2011] UKSC 39

Lucasfilm Ltd v Ainsworth [2009] EWCA Civ 1328

Mazur Media Ltd v Mazur Media GmbH [2004] EWHC 1566 (Ch)

Mecklermedia Corp v DC Congress GmbH [1998] Ch 40

Media C.A.T. v Adams and Others [2011] EWPC 6

Mensah v Jones [2004] EWHC 2699 (Ch)

Miles Platts Ltd v Townroe Ltd [2003] EWCA Civ 145, [2003] 1 All ER 561 (Comm)

Minster Investments Ltd v Hyundai Precision and Industry Co Ltd [1988] 2 Lloyd's Rep 621

Mitsui & Co Ltd v Nexen Petroleum UK Ltd [2005] EWHC 625 (Ch); [2005] 3 All ER 511

Mölnlycke AB v Procter & Gamble Ltd (No. 4) [1992] 1 WLR 1112; [1992] RPC 21

Modus Vivendi Ltd v British Products Sanmex Co Ltd [1996] FSR 790

Norwich Pharmacal Co v Customs & Excise Commissioners [1974] AC 133

Paramount Home Entertainment International Ltd v British Sky Broadcasting [2013] EWHC 3479 (Ch)

Parmiter v Coupland (1840) 6 M & W 105

Pearce v Ove Arup Partnership Ltd [1999] 1 All ER 769 (CA)

Pearce v Ove Arup Partnership Ltd [1997] 2 WLR 779, [1997] Ch 293

Phillips v Eyre [1870] LR 6 QB 1

Polydor Limited v Brown [2005] EWHC 3191

Potter v Broken Hill Pty Co Ltd [1905] VLR 612, affd [1906] 3 CLR 479

PRS v Camelo [1936] 3 All ER 557

Public Relations Consultants Association Limited v the Newspaper Licensing Agency Limited [2013] UKSC 18

R (on the application of) British Telecommunications Plc, Talktalk Telecom Group Plc v Secretary of State for Business, Innovation & Skills [2011] EWCA Civ 232

R (on the application of) British Telecommunications Plc, Talktalk Telecom Group Plc v Secretary of State for Business, Innovation & Skills [2011] EWHC 1021 (Admin)

R v Perrin [2002] EWCA Crim 747, [2002] All ER (D) 359 (Mar)

R v Waddon [2000] All ER (D) 502

Raiffeisen Zentral Bank Österreich AG v Alexander Tranos [2001] IL Pr 9

Red Sea Insurance Co Ltd v Bouygues SA [1995] 1 AC 190

Research in Motion UK Ltd v Visto Corporation [2008] EWCA Civ 153

Rugby Football Union v Consolidated Information Services Limited (Formerly Viagogo Limited) (In Liquidation) [2012] UKSC 55

Rugby Football Union v Vivagogo Ltd [2012] 1 WLR 3333

Rugby Football Union v Vivagogo Ltd [2012] 2 CMLR 3

Rugby Football Union v Vivagogo Ltd [2011] EWHC 764 (QB); [2011] EWCA Civ 1585

Sarrjo v Kuwait Investment Authority [1999] 1 AC 32

Sim v Stretch [1936] 2 All ER 1237

Smith v ADVFN plc [2008] EWCA Civ 518

Sunderland Marine Mutual Insurance Co Ltd v Wiseman [2007] EWHC 1460 (Comm)

Takenaka (UK) Ltd v Frankl [2001] EWCA Civ 348

The Football Association Premier League v British Sky Broadcasting Limited [2013] EWHC 2058 (Ch)

The Lord McAlpine of West Green v Sally Bercow [2013] EWHC 1342 (QB)

Thornton v Telegraph Media Group Ltd [2010] EWHC 1414 (QB)

Totalise plc v Motley Fool Ltd [2002] 1 WLR 1233, [2001] EWCA Civ 1897

Tournier v National Provincial Union Bank of England Ltd [1924] 1 KB 461

Twentieth Century Fox v BT (No 2) [2011] EWHC 2714 (Ch)

Twentieth Century Fox v British Telecommunications plc [2011] EWHC 1981 (Ch)

Union of European Football Association (UEFA) v Euroview [2010] EWHC 1066 (Ch);
[2010] Eu LR 583

Youssouf v Metro-Goldwyn Mayer Pictures Ltd [1934] 50 TLR 581

EU LEGISLATION

Charter:

Charter of Fundamental Rights of the European Union [2000] OJ C364/01

Regulations:

Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast) [2012] OJ L351/1

Council Regulation (EC) 207/2009 of 26 February 2009 on the Community Trade Mark (codified version) [2009] OJ L78/1

Regulation (EC) 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I) [2008] OJ L177/6

Regulation (EC) 1393/2007 of the European Parliament and of the Council of 13 November 2007 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of documents), and repealing Council Regulation (EC) 1348/2000 [2007] OJ L324/79

Regulation (EC) 864/2007 of the European Parliament and of the Council of 11 July 2007 on the law applicable to non-contractual obligations (Rome II) [2007] OJ L199/40

Council Regulation (EC) 6/2002 of 12 December 2001 on Community designs [2002] OJ L3/1

Council Regulation (EC) 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2001] OJ L12/1

Council Regulation (EC) 40/94 of 20 December 1994 on the Community trade mark
[1994] OJ L11/1

Council Regulation (EC) 2100/94 of 27 July 1994 on Community plant variety rights
[1994] OJ L 227/1

Decisions:

Commission Decision 2009/26/EC of 22 December 2008 on the request from the UK to accept Regulation (EC) No 593/2008 of the European Parliament and the Council on the law applicable to contractual obligations (Rome I) [2009] OJ L10/22

Council Decision 2006/325/EC of 27 April 2006 concerning the conclusion of the Agreement between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2006] OJ L120/22

Directives & Corrigenda to Directives:

Council Regulation (EC) 207/2009 of 26 February 2009 on the Community trade mark
[2009] OJ L78/1

Directive 2007/65/EC of the European Parliament and of the Council of 11 December 2007 amending Council Directive 89/552/EC on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities [2007] OJ L332/27

Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights [2006] OJ L372/12

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of

publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54

Corrigendum to Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2009 on the enforcement of intellectual property rights [2004] OJ L195/16

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights [2004] OJ L157/45

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2002] OJ L201/37

Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society [2001] OJ L167/10

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [2000] OJ L178/1

Directive 1996/9/EC of the European Parliament and the Council of 11 March 1996 on the legal protection of databases [1996] OJ L27/20

Directive 95/46/EC of the European Parliament and of the Council 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L281/31

Council Directive 93/83/EEC of 27 September 1993 on the coordination of certain rules concerning copyright and rights related to copyright applicable to satellite broadcasting and cable retransmission [1993] OJ L248/15

Council Directive 92/100/EEC of 19 November 1992 on rental right and lending right and on certain rights related to copyright in the field of intellectual property [1992] OJ L346/61

First Council Directive 89/104/EEC of 21st December 1988 to approximate the laws of the Member States relating to trade marks [1989] OJ L40/1

EU CASES

2014

Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources; and Kärntner Landesregierung* (CJEU (Grand Chamber) 8 April 2014).

Case C-466/12 *Svensson v Retriever Sverige AB* (ECJ (Fourth Chamber) 13 February 2014)

Case C-201/11P *Union des associations européennes de football (UEFA) v European Commission* [2014] 1 CMLR 18

2013

Case C-348/13 *BestWater International GmbH v Mebes, Potsch* (Request for a preliminary ruling from the Bundesgerichtshof (Germany) 25 June 2013)

Case C-614/10 *European Commission v Austria* [2013] 1 CMLR 23

Case C-173/11 *Football Dataco Ltd v Sportradar* [2013] CMLR 29

Case C-607/11 *ITV Broadcasting Ltd v TVCatchup Ltd* [2013] 3 CMLR 1

Case C-279/13 *C More Entertainment AB v Sandberg* (Request for a preliminary ruling from the Högsta domstolen (Sweden) 22 May 2013)

Case C-170/12 *Peter Pinckney v KDG Mediatech AG* [2013] ECDR 15

Case C-523/10 *Wintersteiger AG v Products 4U Sondermaschinenbau GmbH* [2013] CEC 15

2012

Case C-461/10 *Bonnier Audio AB v Perfect Communication Sweden AB* [2012] 2 CMLR 42

Case C-5/11 *Criminal proceedings against Titus Alexander Jochen Donner* (CJEU (Fourth Chamber) 21 June 2012)

Case C-145/10 *Eva-Maria Painer v Standard VerlagsGmbH* [2012] ECDR 6

Case C-135/10 *Società Consortile Fonografici v Marco Del Corso* (ECJ (Third Chamber) 15 March 2012)

Case C-360/10 *Société belge des auteurs compositeurs et éditeurs (SABAM) v Netlog NV* [2012] 2 CMLR 18

2011

Case C-283/10 *Circul Globus București v UCMR – ADA* [2011] ECR I-12031

Joined Cases C-509/09 and C-161/10 *eDate Advertising GmbH v X; Olivier Martinez and Robert Martinez v MGN Ltd* [2011] ECR I-10269

Joined Cases C-403/08 and C-429/08 *Football Association Premier League Ltd v QC Leisure; and Karen Murphy v Media Protection Services Ltd* [2011] ECR I-9083

Case C-323/09 *Interflora Inc, Interflora British Unit v Marks & Spencer plc, Flowers Direct Online Ltd* [2011] ECR I-8625

Case C-324/09 *L'Oréal SA v eBay International AG* [2011] ECR I-6011

Case C-70/10 *Scarlet Extended SA v Société belge des auteurs compositeurs et éditeurs (SABAM)* [2011] ECR I-11959

2010

Joined Cases C-236/08, C-237/08 and C-238/08 *Google France and Google Inc v Louis Vuitton Malletier; Google France v Viaticum Luteciel; Google France v CNRRH* [2010] ECR I-2417

Joined Cases C-585/08 and C-144/09 *Pammer v Reederei Karl Schlüter; Hotel Alpenhof v Oliver Heller* [2010] ECR I-12527

Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] ECR I-11063

2008

Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* [2008] ECR I-271

Case C-73/07 *Tietosuojavaltuutettu v Satakunen Markkinaporssi Oy* [2008] ECR I-9831

2006

Case C-306/05 *Sociedad General Autores y Editores de España (SGAE) v Rafael Hoteles SA* [2006] ECR I-11519

2005

Case C-192/04 *Lagardère Active Broadcast v Société pour la perception de la rémunération équitable (SPRE) and Gesellschaft zur Verwertung von Leistungsschutzrechten mbH (GVL)* [2005] ECR I-7199

Case C-89/04 *Mediakabel BV v Commissariaat voor de Media* [2005] ECR I-4891

Case C-281/02 *Owusu v Jackson (t/a Villa Holidays Bal Inn Villas)* [2005] ECR I-1383

2004

Case C-18/02 *Danmarks Rederiforening, acting on behalf of DFDS Torline A/S v LO Landesorganisationen i Sverige, acting on behalf of SEKO Sjöfolk Facket för Service och Kommunikation* [2004] ECR I-1417

Case C-168/02 *Rudolf Kronhofer v Marianne Maier* [2004] ECR I-6009

2002

Case C-96/00 *Rudolf Gabriel* [2002] ECR I 6367

Case C-167/00 *Verein für Konsumenteninformationen v Karl Heinz Henkel* [2002] ECR I-8111

1998

Case C-51/97 *Réunion Européenne SA v Spliethoff's Bevrachtingskantoor BV* [1998] ECR I-6511

Case C-391/95 *Van Uden Maritime BV (t/a Van Uden Africa Line) v Kommanditgesellschaft in Firma Deco-Line* [1998] ECR I-7091

1995

Case C-68/93 *Fiona Shevill, Ixora Trading Inc, Chequepoint SARL and Chequepoint International Ltd v Presse Alliance SA* [1995] ECR I-415

Case C-364/93 *Marinari v Lloyds Bank plc* [1995] ECR I-2719

1992

Case C-26/91 *Handte v Traitements Mécano-Chimiques des Surfaces* [1992] ECR I-3967

Case C-261/90 *Mario Reichert, Hans-Heinz Reichert and Ingeborg Kockler v Dresdner Bank* [1992] ECR I-2149

1990

Case C-220/88 *Dumez France SA and Tracoba SARL v Hessische Landesbank* [1990] ECR I-49

1988

Case 189/87 *Kalfelis v Bankhaus Schröder, Münchmeyer, Hengst and Co* [1988] ECR 5565

1980

Case 56/79 *Zelger v Salinitri* [1980] ECR 89

1979

Case 143/78 *De Cavel v De Cavel* [1979] ECR 1055

1976

Case 21/76 *Handelskwekerij G J Bier BV v Mines de Potasse d'Alsace SA* [1976] ECR
1735

SUNDRY OTHER EU DOCUMENTS

EU Agreements, Conventions & Treaties:

1968 Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters [1972] OJ L299/32

1980 Rome Convention on the law applicable to contractual obligations (consolidated version) [1998] OJ C27/34

80/934/EEC Convention on the Law Applicable to Contractual Obligations (opened for signature in Rome 1980, entered into force 1991, consolidated version published in 2005) [1980] OJ L266/1

Agreement 89/695/EEC relating to Community patents [1989] OJ L401/1

Agreement between the European Community and the Kingdom of Denmark on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2005] OJ L299/62

Agreement between the European Community and the Kingdom of Denmark on the service of judicial and extrajudicial documents in civil or commercial matters [2008] OJ L331/21

Consolidated Version of the Treaty establishing the European Community (TEC) [2002] OJ C325/33

Consolidated Version of the Treaty on the Functioning of the European Union (TFEU) [2008] OJ C115/47

Convention on jurisdiction and the enforcement of judgments in civil and commercial matters (consolidated version) [1998] OJ C27/1

European Convention relating to questions on Copyright Law and Neighbouring Rights in the Framework of Transfrontier Broadcasting by Satellite 1994

Lugano Convention on jurisdiction and the enforcement of judgments in civil and commercial matters (1988, extended 2007) [2007] OJ L339/3

Draft Framework Decisions:

Council of the European Union, 'Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism' Council doc 8958/04 CRIMORG 36 TELECOM 82 (28 April 2004)

Council of the European Union, 'Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism' Council doc 13353/04 CRIMORG 79 TELECOM 126 (14 October 2004)

Green Papers & Follow-up:

Commission, 'Green Paper: Copyright and Related Rights in the Information Society' COM (1995) 382 final

Commission, 'Follow-up to the Green Paper on Copyright and Related Rights in the Information Society' COM (1996) 568 final

Commission, 'Green Paper: Copyright in the Knowledge Economy' COM (2008) 466/3

Proposals:

Commission, 'Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)' COM (2012) 11 final

Commission, 'Proposal for a Regulation of the European Parliament and the Council on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Recast)' COM (2010) 748 final

Commission, 'Proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights' COM (2005) 276 final

Commission, 'Proposal for a Regulation of the European Parliament and the Council on the law applicable to contractual obligations (Rome I)' COM (2005) 650 final

Commission, 'Proposal for a regulation of the European Parliament and the Council on the law applicable to non-contractual obligations ("Rome II")' COM (2003) 427 final

Opinions:

Case C-314/12 *UPC Telekabel Wien v Constantin Film*, Opinion of AG Cruz Villalón (26 November 2013)

Case C-173/11 *Football Dataco v Sportradar GmbH*, Opinion of AG Cruz Villalón (21 June 2012)

Opinion 1/03 of the Court of Justice of the European Communities of 7 February 2006 on the Competence of the Community to conclude the new Lugano Convention on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [2006] ECR I-1145

Case C-281/02 *Owusu v Jackson* [2005] ECR I-1383, Opinion of AG Léger

Case C-167/00 *Verein für Konsumenteninformation v Karl Heinz Henkel* [2002] ECR I-8111, Opinion of AG Jacobs

Case C-51/97 *Réunion Européenne SA v Spliethoff's Bevrachtingskantoor BV* [1998] ECR I-6511, Opinion of AG Cosmas

Sundry (Press releases etc):

Dusollier S, Depreeuw S, Hubin J-B, Coppens F, de Francquen A, 'Study on the Application of Directive 2001/29/EC on Copyright and Related Rights in the Information Society' (*European Commission*, 2013)

<http://ec.europa.eu/internal_market/copyright/docs/studies/131216_study_en.pdf>

accessed 5 May 2014

European Commission, 'Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of their data and to cut costs for businesses'

(IP/12/46, 25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm>
accessed 16 April 2014

European Commission, 'Withdrawal of Obsolete Commission Proposals' [2010] OJ
C252/9

Jenard P, Report on the Convention on Jurisdiction and the Enforcement of Judgments
in Civil and Commercial Matters [1979] OJ C59/1

Kuner C, Burton C, Bloemen-Patberg A, Konarski X, and Hall P, 'Study on Online
Copyright Enforcement and Data Protection in Selected Member States - Netherlands,
Poland, United Kingdom' (*European Commission - DG Internal Market and Services*,
April 2010) <http://ec.europa.eu/internal_market/iprenforcement/docs/study-online-enforcement_042010_en.pdf> accessed 6 May 2014

Law Commission, *Defamation and the Internet – A Preliminary Investigation* (Scoping
Study No 2, December 2002)

OHIM, 'European Citizens and Intellectual Property: Perception, Awareness and
Behaviour' (November 2013) <[https://oami.europa.eu/tunnel-
web/secure/webdav/guest/document_library/observatory/documents/IPContributionStud
y/25-11-2013/european_public_opinion_study_web.pdf](https://oami.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/IPContributionStudy/25-11-2013/european_public_opinion_study_web.pdf)> accessed 21 May 2014

Protocol on the Settlement of Litigation concerning the Infringement and Validity of
Community Patents [1989] OJ L401/34

NON-UK LEGISLATION

Australia:

Copyright Act 1968

Interactive Gambling Act 2001

New Tax System (Goods and Services) Act 1999 (no 55,1999)

Belgium:

Code de droit international privé (Code of Private International Law) (2004)

Canada:

Copyright Act (RSC, 1985, c C-42)

Federal Courts Act (RSC, 1985, c F-7)

Federal Courts Rules (SOR/98-106)

Personal Information Protection and Electronic Documents Act (SC 2000, c 5)

Germany:

Bundesdatenschutzgesetz (Federal Data Protection Act) (1990, redrafted 2003)

Medienstaatsvertrag (Interstate Media Services Agreement)

Telekommunikationsgesetz (Telecommunications Act) (2004)

Telemediengesetz (Teleservices Act) (2007)

Zivilprozessordnung (Code of Civil Procedure) (1877, redrafted 2005)

Italy:

Private International Law Act 1995

Netherlands:

Conflict of Laws on Torts Act (2001)

Republic of Korea:

Private International Law Act 2001

Switzerland:

Bundesgesetz über das Internationale Privatrecht (Federal Private International Law Act) (SR 291, 1987)

USA:

Children's Online Privacy Protection Act (15 USC (§§ 6501-6506) Pub L 105-277, 112 Stat 2581-728, enacted 1998)

Digital Millennium Copyright Act (1998)

Lanham (Trademark) Act (15 USC, ch 22 (§§ 1051-1141n) Pub L 79-489, 60 Stat 427, enacted 1946)

Restatement (Second) of Torts (1976)

Uniform Foreign Money Judgment Recognition Act (NY CPLR, art 53 (§§ 5301-5309))

Uniform Single Publications Act (FSMC, title 6, ch 11 (§§ 1101 et seq) 1952)

NON-UK CASES

Austria:

OGH 24.04.2002, GRUR Int 2002, 265 ('Red Bull' case)

OGH 28.9.1993, 4 Ob 125/93, GRUR Int 1993, 638 = MR 1994, 26 ('Adolf Loos-Werke II')

OGH 18.9.1990, 4 Ob 139/90, GRUR Int 1991, 650 = IPRax 1991, 347 = MR 1991, 112

OGH 17.6.1986, 4 Ob 309/86, GRUR Int 1986, 728 = ÖBl 1986, 132 = SZ 59/100 = JBl 1986, 655 = MR 1986 H4, 20 (*Hotel-Video*)

OGH 14.1.1986, 4 Ob 408/85, GRUR Int 1986, 735 = ÖBl 1986, 73 ('Hotel Sacher')

OGH 28.6.1983, 4 Ob 345/82, GRUR Int 1984, 453 = ÖBl 1983, 162 = SZ 56, 107 ('Attco/ATCO')

Australia:

Cooper v Universal Music Australia Pty Ltd [2006] FCAFC 187

David Syme Ltd v Grey (1992) 115 ALR 247

Dow Jones & Company Inc v Gutnick [2002] HCA 56

Gutnick v Dow Jones & Co Inc [2001] VSC 305

Spotless Group v Proplast [1987] 10 IPR 668

TVBO Production Ltd v Australia Sky Net Pty Ltd [2009] FCA 1132

Canada:

Beals v Saldanha, [2003] 3 SCR 416, [2003] SCC 72

BMG Canada Inc v John Doe [2004] FC 488, [2004] 3 FCR 241

BMG Canada Inc v John Doe [2005] FCA 193, [2005] 4 RCF 81

Canada (Human Rights Commission) v Canadian Liberty Net, [1998] 1 SCR 626

Ford Aquitaine Industries SAS v Canmar Pride (The), [2005] 4 FCR 441, [2005] FC 431

Holt Cargo Systems Inc v ABC Containerline NV (Trustees of), [2001] 3 SCR 907, [2001] SCC 90

Hunt v T&N plc, [1993] 4 SCR 289

Libman v The Queen, [1985] 2 SCR 178

Morguard Investments Ltd v De Savoye, [1990] 3 SCR 1077

Muscutt v Courcelles [2002] OJ 2128, [2002] 60 OR (3d) 20

Perfect 10, Inc v Google Inc and Google Canada Corporation, [2011] FC 348

Society of Composers, Authors and Music Publishers of Canada v Canadian Association of Internet Providers, [2004] 2 SCR 427, [2004] SCC 45

Spar Aerospace Ltd v American Mobile Satellite Corp, [2002] 4 SCR 205, [2002] SCC 78

Tolofson v Jensen, [1994] 3 SCR 1022

Unifund Assurance Co v Insurance Corp of British Columbia, [2003] 2 SCR 63, [2003] SCC 40

France:

Castellblanch SA v Champagne Louis Roederer SA [2004] IL Pr 41

Haftpflichtverband der Deutschen Industrie Versicherungsverein auf Gegenseitigkeit (HDI) v Soci t e AXA France IARD [2007] IL Pr 28, Cour de Cassation

Ideal Clima SpA v SA Ideal Standard Gaz Pal [1982], Somm, 378; D Series I-5.3-B13, Cour d'Appel Paris

International League Against Racism & Anti-Semitism (LICRA), French Union of Jewish Students (UEJF) v Yahoo! Inc, Yahoo France, Interim Court Order, 20 November 2000, Tribunal de Grande Instance de Paris (Country Court of Paris)

Jean Lamore v Universal City Studios Inc (2007) 212 RIDA 260, Cour de Cassation, first civil chamber

Radio P riph riques v SNEP (2009) 144 RIDA 215, Cour d'Appel de Paris

SAIF v Google doc no 05/12117, Civil Court of Paris

Sisro v Ampersand Software BV [2003] RCDIP 440, [2003] GRUR Int 75, Cour de Cassation, first civil chamber

Wegmann v Soci t  Elsevier Science Ltd [1997] IL Pr 760, Cour de Cassation

Germany:

OVG Nordrhein-Westfalen 02.07.2010, 13 B 646/10

VGH Bayern 20.11.2008, 10 CS 08.2399

OVG Th ringen 03.12.2008, 3 EO 565/07

BGH GRUR 2003, 328 ('Felsberg Transmitter')

LG D sseldorf, 4 O 198/97, GRUR Int 1999, 775 ('Impstoff II')

IIC 1995, 573 ('Folgerecht')

Oberster Gerichtshof 28.5.1991, 4 Ob 19/91; OGH ÖBl 1991, 181; GRUR Int 1991, 920 ('Tele Uno III')

German Federal Supreme Court, BGH I ZR 201/86, EEC 1988, 415; NJW 1988, 1466; GRUR 1988, 483 (Re Jurisdiction in Tort and Contract)

IIC 1977, 276 ('Hummel Christmas Plate')

BGHZ 41, 84 ('Maja')

BGHZ 49, 331 ('Vorán')

Reich Supreme Court 1936 JW 1291

Hong Kong:

Cinepoly Records Co Ltd v Hong Kong Broadband Network Ltd [2006] 1 HKLRD 255, HCMP 2487 (2005)

Netherlands:

NV Gebr Van Zijverden v GF Mens [1973] BIE 99

Hof Arnhem (Court of Appeal Arnhem), 26 June 1993, [1995] BIE 44, [1995] NIPR 555 (*Relo v Fumitex*)

Hoge Raad (Supreme Court) 27 January 1995, [1995] NJ 669, [1995] NIPR 388 (*Bigott-Batco v Doucal*)

New Zealand:

Atkinson Footwear Ltd v Hodgkin International Services Ltd (1995) 31 IPR 186

KK Sony Computer Entertainment v Van Veen (2006) 71 IPR 179

Norway:

Saba Mölnlycke AS v Procter & Gamble Scandinavia Inc [1997] IL Pr 704

Republic of Ireland:

EMI Records (Ireland) Limited v Data Protection Commissioner [2013] IESC 34

EMI Records & Ors v Eircom Ltd [2010] IEHC 108

EMI Records Ltd v Eircom Ltd [2005] 4 IR 148

Eoin McKeogh v John Doe and Others (Record No. 2012/254P, 16th May 2013)

Schmidt v Home Secretary [1995] 1 ILRM 301

Singapore:

Odex Ptd Ltd v Pacific Internet Ltd [2007] SGDC 248

Odex Ptd Ltd v Pacific Internet Ltd [2008] SGHC 35

South Africa:

Gallo Africa Ltd v Sting Music (Pty) Ltd [2010] ZASCA 96, [2011] 1 All SA 449 (SCA)

USA:

ALS Scan, Inc v Digital Service Consultants, Inc, 293 F 3d 707 (4th Cir 2002)

Amberson Holdings LLC v Westside Story Newspaper, 110 F Supp 3d 332 (DNJ 2000)

Asahi Metal Industry Co Ltd. v Superior Court of California, 480 US 102 (1987)

Bensusan Restaurant Corp v King, 937 F Supp 295 (SDNY 1996)

Bochan v La Fontaine, 68 F Supp 2d 692 (ED Va 1999)

Boosey & Hawkes Music Pubs v The Walt Disney Co, 145 F 3d 481 (2nd Cir 1998)

Burger King Corp v Rudzewicz, 471 US 462; 105 S Ct 2174 (1985)

Calder v Jones, 465 US 783 (1984)

Columbia Pictures Industries, Inc v Fung, 2009 WL 635591 (CD Cal 2009)

CompuServe, Inc v Patterson, 89 F 3d 1257 (6th Cir 1996)

Cybersell, Inc v Cybersell, Inc, Webhorizons Inc, Websolvers, Inc, 130 F 3d 414 (9th Cir 1997)

Euromarket Designs Inc. v Crate & Barrel Ltd, 96 F Supp 2d 824 (ND III 2000)

Firth v State of New York, 706 NYS 2d 835 (2000)

Hanson v Denckla, 357 US 235 (1958)

Hageseth v Superior Court of San Mateo County, 150 Cal App 4th 1399; 59 Cal Rptr 3d 385; Cal Daily Op Service 5647 (2007)

Hy Cite Corporation v BadBusinessBureau.com, [2004] WL 42641 (WD Wis 2004)

Inset Systems, Inc v Instruction Set, 967 F Supp 161 (D Conn 1996)

International Shoe Co v State of Washington, 326 US 310 (1945)

Itar-Tass Russian News Agency v Russian Kurier, Inc, 153 F 3d 82 (2d Cir 1998)

Johnson v Microsoft Corp, C06-0900RAJ-WD Wa 06/23/09, 2009 WL 17934400

Kauffman Racing Equipment, LLC v Roberts, 126 Ohio St 3d 81, 930 NE 2d 784 (Ohio 2010)

Keeton v Hustler Magazine, Inc, 465 US 770 (1984)

Los Angeles News Service v Conus Communications Co, 969 F Supp 579 (CD Cal 1997)

Los Angeles News Serv v Reuters TV Int'l Ltd, 149 F 3d 987 (9th Cir 1998)

Mar-Eco v T&R and Sons Towing and Recovery, 837A 2d 512 (Pa Super 2003)

Marits, Inc v Cybergold, 947 F Supp 1328 (ED Mo 1996)

Mitan v Davis, 243 F Supp 2d 719 (WD Ky 2003)

National Federation of the Blind v Target Corp, 452 F Supp 2d 946, 961 et seq (ND Cal 2006)

National Football League v Prime Time 24 Joint Venture, 211 F 3d 10 (2d Cir 2000)

Nissan Motors Co Ltd & Nissan North America, Inc v Nissan Computer Corporation, 89 F Supp 2d 1154 (CD Cal 2000)

Penguin Group (USA) Inc v American Buddha, 640 F 3d 497 (2d Cir NY 2011), docket no 09-1739-cv

Perfect 10 Inc v Google Inc 416 F Supp 2 d 828 (CD Cal 2006)

Revell v Lidov, 317 F 3d 467 (5th Cir 2002)

SARL Louis Feraud International v Viewfinder Inc, 406 F Supp 2d 274 (SDNY 2005)

SARL Louis Feraud International v Viewfinder Inc, 489 F3d 474 (2nd Cir 2007)

Sheldon v Metro-Goldwyn Pictures Corp, 106 F 2d 45 (2d Cir 1939)

State of New Jersey v Shirley Reid, 194 NJ 386, 954 A2d 503 (NJ 2008)

Subafilms Ltd v MGM-Pathe Communications Co, 24 F 3d1088 (9th Cir 1994)

The Traditional Cat Association v Gilbreath, 13 Cal Rptr 3d 353 (Cal Crt App 2004)

Toys R US Inc v Step Two SA, 318 F 3d 446 (3rd Circuit 2003)

Twentieth Century Fox Film Corp v iCrave TV; National Football League v TVRadioNow Corp 2000 WL 255989 (WD Pa Feb 8, 2000), 53 USPQ2d (BNA) 1831 (settled on 28 February 2000)

Update Art, Inc v Modiin Publishing, Ltd, 843 F 2d 67 (2d Cir 1988)

Van Buskirk v New York Times Co, No 99 Civ 4265 (MBM), 2000 WL 1206732; 28 Media L Rep 2525 (SDNY 2000); 325 F 3d 87(2nd Cir 2003)

Vanity Fair Mills, Inc v T Eaton Co Ltd, 234 F 2d 633 (2d Cir 1956), 352 US 871 (1956)

Voda v Cordis Corp, 476 F 3d 887 (Fed Cir 2007)

Westcode v RBE Electronics, 2000 US Dist LEXIS 815 (ED Pa Feb 1, 2000)

World-Wide Volkswagen v Woodson, 444 US 286 (1980)

Yahoo!, Inc v LICRA, 169 F Supp 2d 1181 (ND Cal 2001)

Young v New Haven Advocate, 315 F 3d 256 (4th Cir 2002)

Zippo Manufacturing Company v Zippo Dot Com, Inc, 952 F Supp 1119; 42 USPQ 2D 1062 (DC WD Pa 1997)

INTERNATIONAL CONVENTIONS AND TREATIES

Berne Convention for the Protection of Literary and Artistic Works 1886 (completed at Paris 1896, revised at Berlin 1908, completed at Berne 1914, revised at Rome 1928, at Brussels 1948, at Stockholm 1967, at Paris 1971, amended 1979)

Convention on Cybercrime (open for signature in Budapest 2001)

Convention on the recognition and enforcement of foreign judgments in civil and commercial matters 1971

Hague Convention on Choice of Court Agreements 2005

Paris Convention for the Protection of Industrial Property 1883 (revised at Brussels 1900, at Washington 1911, at The Hague 1925, at London 1934, at Lisbon 1958, at Stockholm 1967, amended 1979)

Trade-Related Aspects of Intellectual Property Rights (signed in Marrakesh 1994)

Universal Copyright Convention (adopted at Geneva 1952, entry into force 1955, revised at Paris 1971)

WIPO Copyright Treaty (adopted in Geneva 1996)

WIPO Performances and Phonograms Treaty (WPPT) (adopted in Geneva 1996)

BOOKS

ALI, *Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes* (ALI Publishers 2008)

Basedow J, Drexl J, Kur A and Metzger A (eds), *Intellectual Property in the Conflict of Laws* (Mohr Siebeck 2005)

Bellia P, Schiff Berman P and Post D, *Cyberlaw, Problems of Policy and Jurisprudence in the Information Age* (3rd edn, Thomson West 2007)

Bently L and Sherman B, *Intellectual Property Law* (3rd edn, OUP 2009)

Boele-Woelki K and Kessedjian C (eds), *Internet: Which Court Decides?, Which Law Applies? Quel tribunal decide? Quel droit s'applique?* (1st edn, Kluwer Law International 1998)

Briggs A, *The Conflict of Laws* (3rd edn, OUP 2013)

Briggs A, *The Conflict of Laws* (2nd edn, OUP 2008)

Chalmers J, *The Economist Pocket Telecommunications: The Essentials of Telecommunications Explained from A to Z* (Economist Books 1995)

Clarkson CMV and Hill J, *The Conflict of Laws* (4th edn, OUP 2011)

Clarkson CMV and Hill J, *Jaffey on the Conflict of Laws* (2nd edn, LexisNexis UK 2002)

Collins L, Briggs A, Harris J, McClean JD, McLachlan C and Morse CGJ (eds), *Dicey, Collins and Morris: The Conflict of Laws*, vol 1 (14th edn, Sweet & Maxwell 2006)

Collins L, Briggs A, Harris J, McClean JD, McLachlan C and Morse CGJ (eds), *Dicey, Collins and Morris: The Conflict of Laws*, vol 2 (14th edn, Sweet & Maxwell 2006)

Collins L, Briggs A, Harris J, McClean JD, McLachlan C and Morse CGJ (eds), *Dicey, Morris & Collins on The Conflict of Laws* (1st supp, 14th edn, Sweet & Maxwell 2007)

Cornish W, Llewelyn D and Aplin T, *Intellectual Property: Patents, Copyright, Trademarks and Allied Rights* (8th edn, Sweet & Maxwell 2013)

Desbois H, Françon A and Kerever A, *Les conventions internationales du droit d'auteur et des droits voisins* (Dalloz 1976)

Dickinson A, *The Rome II Regulation – The Law Applicable to Non-Contractual Obligations* (1st edn, OUP 2008)

Dickinson A, *The Rome II Regulation – The Law Applicable to Non-Contractual Obligations* Updating Supplement (1st edn, OUP 2010)

Drexler J and Kur A (eds), *Intellectual Property and Private International Law – Heading for the Future (IIC Studies)* (Hart Publishing 2005)

Fawcett JJ, Carruthers J and North P, *Cheshire, North & Fawcett: Private International Law* (14th edn, OUP 2008)

Fawcett JJ and Torremans P, *Intellectual Property and Private International Law* (2nd edn, OUP 2011)

Garner BA (ed), *Black's Law Dictionary* (8th edn, West Publishing 2004)

Goldstein P and Hugenholtz PB, *International Copyright: Principles, Law and Practice* (3rd edn OUP 2013)

Goldstein P, *International Copyright: Principles, Law and Practice* (OUP 2001)

- Gottschalk E, Michaels R, Ruhl G, and von Hein J (eds), *Conflict of Law in a Globalised World* (1st edn, CUP 2007)
- Gringras C and Todd E, *Gringras: The Laws of the Internet* (3rd edn, Tottel 2008)
- Hartley TC, *International Commercial Litigation, Text, Cases and Materials on Private International Law* (1st edn, CUP 2009)
- Hill J, *Cross-Border Consumer Contracts* (Oxford University Press 2008)
- Hörnle J and Zammit B, *Cross Border Online Gambling Law and Policy* (Edgar Elgar 2010)
- Huard G, *Étude sur les modifications apportées à la Convention de Berne par la conférence réunie à Paris du 15 avril au 1^{er} mai, 1896* (Pichon 1897)
- Jay R, *Data Protection Law & Practice* (3rd end, Sweet & Maxwell 2007)
- Juenger FK, *Selected Essays on the Conflict of Laws (Transnational Classics in International Law, 1)* (1st edn, Transnational Pub 2000)
- Kono T (ed), *Intellectual Property and Private International Law – Comparative Perspectives* (Hart Publishing 2012)
- Kulesza J, *International Internet Law* (1st edn, Routledge 2012)
- Ku RSR and Lipton J, *Cyberspace Law – Cases and Materials* (3rd edn, Wolters Kluwer 2010)
- Laughlin SK, *The Law of the United States Territories and Affiliated Jurisdictions* (Lawyers Cooperative Publishing 1995)
- Leible S and Ohly A (eds), *Intellectual Property and Private International Law* (1st edn, Mohr Siebeck 2009)

- Lessig L, *Code and Other Laws of Cyberspace* (1st edn, Basic Books 1999)
- Lloyd I, *Cyber Law in the United Kingdom* (Kluwer Law International 2010)
- Lloyd IJ, *Information Technology Law* (6th edn, OUP 2011)
- Lord Collins of Mapesbury, Morse CGJ, McClean D, Briggs A, Harris J, McLachlan C, Dickinson A, McEleavy P (eds), *Dicey, Collins and Morris: The Conflict of Laws*, vol 1 (15th edn, Sweet & Maxwell 2012)
- Lord Collins of Mapesbury, Morse CGJ, McClean D, Briggs A, Harris J, McLachlan C, Dickinson A, McEleavy P (eds), *Dicey, Collins and Morris: The Conflict of Laws*, vol 2 (15th edn, Sweet & Maxwell 2012)
- Lowenfeld AF, Silberman LJ (eds), *The Hague Convention on Jurisdiction and Judgments – Records of the Conference Held at New York University School of Law on the Proposed Convention, April 30 – May 1, 1999* (Juris Publishing 2001)
- Lucas A and Lucas HJ, *Traité de la propriété littéraire et artistique* (2nd edn, Litec 2001)
- Mastroianni R, *Diritto Internazionale e Diritto d’Autore* (A Giuffrè 1997)
- McBride NJ and Bagshaw R, *Tort Law* (4th ed, Pearson 2013)
- McClean D and Beevers K, *Morris - The Conflict of Laws* (6th edn, Sweet & Maxwell 2005)
- McClean D and Abou-Nigm VR, *Morris - The Conflict of Laws* (8th edn, Sweet & Maxwell 2012)
- Murray A, *Information Technology Law – The Law and Society* (2nd edn, Oxford University Press 2013)

Neill B, Rampton R, Rogers H, Atkinson T, Eardley A, *Duncan and Neill on Defamation* (3rd edn, LexisNexis Butterworths 2009)

Parkes R, Mullis A, Busuttill G, *Gatley on Libel and Slander* (12th edn, Sweet & Maxwell 2013)

Reed C, *Internet Law: Text and Materials* (2nd edn, CUP 2004)

Reinbothe J and von Lewinski S, *The WIPO Treaties 1996* (Butterworths LexisNexis 2002)

Ricketson S and Ginsburg J, *International Copyright & Neighbouring Rights - The Berne Convention and Beyond*, vol I (2nd edn, OUP 2006)

Ricketson S and Ginsburg J, *International Copyright & Neighbouring Rights - The Berne Convention and Beyond*, vol II (2nd edn, OUP 2006)

Rowland D, Kohl U and Charlesworth A, *Information Technology Law* (4th edn, Routledge 2012)

Schack H, *Zur Anknüpfung des Urheberrechts im internationalen Privatrecht* (Duncker & Humblot 1979)

Smith GJH, *Internet Law and Regulation* (4th edn, Sweet & Maxwell 2007)

Spang-Hanssen HS, *Cyberspace Jurisdiction in the U.S. -The International Dimension of Due Process* (Institutt for rettsinformatikk 2001)

Spang-Hanssen H, *Cyberspace & International Law on Jurisdiction: Possibilities of Dividing Cyberspace into Jurisdiction with Help of Filters and Firewall Software* (DJØF Publishing 2004)

Sterling JAL, *World Copyright Law* (3rd edn, Sweet & Maxwell 2008)

Stewart SM, *International Copyright and Neighbouring Rights* (2nd edn, Butterworths Law 1989)

Strowel A (ed), *Peer-to-peer file sharing and secondary liability in copyright law* (Edward Elgar 2009)

Svantesson DJB, *Private International Law and the Internet* (2nd edn, Wolters Kluwer 2012)

Torremans P, *Holyoak and Torremans Intellectual Property Law* (7th edn, OUP 2013)

Tritton G, *Intellectual Property in Europe* (3rd edn, Sweet & Maxwell 2008)

Ulmer E, *Intellectual Property Rights and the Conflict of Laws: a study carried out for the Commission of the European Communities, Directorate-General for Internal Market and Industrial Affairs* (Kluwer 1978)

van Eechoud M, *Choice of Law in Copyright and Related Rights – Alternatives to the Lex Protectionis (Information Law Series)* (1st edn, Kluwer Law International 2003)

Vermeulen G (ed), *EU quality standards in support of the fight against trafficking in human beings and sexual exploitation of children (Exploratory study of the potential and feasibility of self-regulation or public-private co-operation)* (Maklu 2007)

von Bar C, *Internationales Privatrecht*, vol II (2nd edn, CH Beck 1991)

Wadlow C, *Enforcement of Intellectual Property in European and International Law* (Sweet & Maxwell 1998)

Wang FF, *Internet Jurisdiction and Choice of Law: Legal Practices in the EU, US and China* (1st edn, Cambridge University Press 2010)

Weintraub RJ, *Commentary on the Conflict of Laws* (4th edn, Foundation Press 2001)

CONTRIBUTIONS TO EDITED BOOKS

Bernstein M, 'A Global Network in a Compartmentalised Legal Environment' in Boele-Woelki K and Kessedjian C (eds), *Internet: Which Court Decides?, Which Law Applies? Quel tribunal décide? Quel droit s'applique?* (1st edn, Kluwer Law International 1998)

Dessemontet F, 'L'harmonisation du droit applicable aux contrats de licence' in Stoffel WA and Volken P (eds), *Conflict et harmonisation: mélanges en l'honneur d'Alfred E. von Overbeck à l'occasion de son 65^{ème} anniversaire* (Éditions Universitaires Fribourg Suisse 1990)

Díaz C and Preneel B, 'Reasoning about the Anonymity Provided by Pool Mixes that Generate Dummy Traffic' in Fridrich JJ (ed), *Information Hiding, 6th International Workshop, LNCS 3200* (Springer-Verlag 2004)

Díaz C and Preneel B, 'Taxonomy of Mixes and Dummy Traffic', in IFIP (ed), *3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems* (Kluwer Academic Publishers 2004)

Grosheide W, 'Experiences in the Field of Intellectual Property' in Boele-Woelki K and Kessedjian C (eds), *Internet, Which Court Decides? Which Law Applies? (Quel tribunal décide? Quel droit s'applique?)* (1st edn, Kluwer Law International 1998)

Holznagel B and Sonntag M, 'A Case Study: The Janus Project' in Nicoll C, Prins JEJ and van Dellen MJM (eds), *Digital Anonymity and the Law: Tensions and Dimensions - Information Technology & Law Series 2* (1st edn, Asser Press 2003)

Hörnle J, 'The Jurisdictional Challenge of the Internet' in Edwards L and Waelde C (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009)

Juenger FK, 'A Shoe Unfit for Globetrotting' in Juenger FK (ed), *Selected Essays on the Conflict of Laws (Transnational Classics in International Law, 1)* (1st edn, Transnational Pub 2000)

Juenger, F, 'The Problem with Private International Law' in Basedow J, Meier I, Schnyder AK, Einhorn T and Girsberger D (eds), *Private International Law in the*

International Arena: From National Conflict Rules Towards Harmonization and Unification - Liber Amicorum Kurt Siehr (1st edn, Asser Press 2000)

Kur A, 'Are there any common European principles of Private International Law with regard to Intellectual Property?' in Leible S and Ohly A (eds), *Intellectual Property and Private International Law* (1st edn, Mohr Siebeck 2009)

Longworth E, 'The possibilities for a legal framework for cyberspace including a New Zealand perspective' in de Padirac B (ed), *The International Dimensions of Cyberspace Law (Law of Cyberspace Series, vol 1)* (Ashgate Pub Ltd 2001)

MacQueen HL, "'Appropriate for the Digital Age"? Copyright and the Internet: 1. Scope of Copyright' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009)

Metzger A, 'Jurisdiction in Cases Concerning Intellectual Property Infringements on the Internet – Brussels I Regulation, ALI principles and Max Planck Proposals' in Leible S and Ohly A (eds), *Intellectual Property and Private International Law* (1st edn, Mohr Siebeck 2009)

Nicoll C, 'Concealing and Revealing Identity on the Internet' in Nicoll C, Prins JEJ and van Dellen MJM (eds), *Digital Anonymity and the Law: Tensions and Dimensions - Information Technology & Law Series 2* (1st edn, Asser Press 2003)

Nuyts A, 'Suing at the Place of Infringement: The Application of Article 5 (3) of Regulation 44/2001 to IP Matters and Internet Disputes' in Nuyts A (ed), *International Litigation in Intellectual Property and Information Technology* (Kluwer Law International 2008)

Nygh P, 'The Preliminary Draft Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters' in Borchers PJ and Zekoll J (eds), *International Conflict of Laws for the Third Millennium – Essays in Honor of Friedrich K Juenger* (Transnational Pub 2001)

Pertegás M, 'Intellectual Property and Choice of Law Rules' in Malatesta A (ed), *The Unification of Choice of Law Rules on Torts and Other Non-Contractual Obligations in Europe* (CEDAM 2006)

Pontier JA, 'Onrechtmatige Daad' in Vlas P (ed), *Praktijkreeks IPR, No 16* (Kluwer 2001)

Quadvlieg AA, 'Een multiple personality syndrome in het IPR: de identificatie van de auteursrechthebbende' in Kortmann SCJJ and Struycken AVM, *Op recht: bundle opstellen, aangeboden aan prof. mr. A.V.M. Struycken ter gelegenheid van zijn zilveren ambtsjubileum aan de Katholieke Universiteit Nijmegen* (WEJ Tjeenk Willink 1996)

Rauhofer J, 'The Retention of Communications Data in Europe and the UK' Edwards L and Waelde C (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009)

Stromholm S, 'Preface' in Basedow J, Drexl J, Kur A and Metzger A (eds), *Intellectual Property in the Conflict of Laws* (Mohr Siebeck 2005)

Taubman A, 'International Governance and the Internet' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet* (3rd edn, Hart Publishing 2009)

Thornburgh D and Lin HS, 'A Global Internet' in Thornburgh D and Lin HS (eds), *Youth, Pornography and the Internet* (National Academy Press 2002)

Torremans P, 'Private International Law Aspects of IP – Internet Disputes' in Edwards L and Waelde C (eds), *Law and the Internet: a Framework for Electronic Commerce* (2nd edn, Hart Publishing 2000)

ENCYCLOPEDIA

Lloyd I and Saxby S, 'Information Technology Law' in Lord Mackay of Clashfern (ed), *Halsbury's Laws of England*, Vol 57 (5th edn, LexisNexis 2012)

JOURNAL ARTICLES

Adams WA, 'Intellectual Property Infringement in Global Networks: The Implications of Protection Ahead of the Curve' (2002) 10 Int J Law Info Tech 71

Akdeniz Y, 'Case Analysis of League Against Racism & Antisemitism (LICRA), French Union of Jewish Students (UEJF), v Yahoo! Inc, (USA), Yahoo France, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order, 20 November, 2000' (2001) 1 Electron Bus Law Rep 110

Alexander I, 'All change for the digital economy: some observations from the history of copyright' (2010) 28 Copyright Reporter: Journal of the Copyright Society of Australia 215

Association Littéraire et Artistique Internationale, 'Report and Opinion on the making available and communication to the public in the internet environment: focus on linking techniques on the internet' (2014) 36 EIPR 149

Basedow J, 'The communitarization of the conflict of laws under the Treaty of Amsterdam' (2000) 37 CMLR 687

Beaumont P, 'Hague Choice of Court Agreements Convention 2005: Background, Negotiations, Analysis and Current Status' (2009) 5 JourPIL 125

Bigos O, 'Jurisdiction over Cross-Border Wrongs on the Internet' (2005) 54 ICLQ 585

Boytha G, 'Some Private International Law Aspects of the Protection of Authors' (1988) 24 Copyright 399

Burk DL, 'Patents in cyberspace: Territoriality and infringement on global computer networks' (1993) 68 TLR 1

Calliess GP, 'Value-Added Norms, Local Litigation, and Global Enforcement: why the Brussels Philosophy failed in The Hague' (2004) 5 German L J 1399

Chan Y, Thant Z, Zimmerman R, and Parsley LLL, 'Towards an Integrated System to Handle Garnishment Forms for Garnishees, Judgment Debtors, Judgment Creditors, and the Courts' (2006) 14 Int J Law Info Tech 242

Claessens J, Díaz C, Goemans C, Dumortier J, Preneel B and Vandewalle J, 'Revocable anonymous access to the Internet' (2003) 13 Journal of Internet Research 242

CLIP, 'Comments on the European Commission's Proposal for a Regulation on the Law Applicable to Contractual Obligations ("Rome I") of 15 December 2005 and the European Parliament Committee on Legal Affairs' Draft Report on the Proposal of 22 August 2006' (2007) 38 IIC 471

Creech RL, 'Dow Jones and the Defamatory Defendant Down Under: A Comparison of Australian and American Approaches to Libelous Language in Cyberspace' (2004) 22 JMarshall JComputer & InfoL 553

Czychowski C and Nordemann JB, 'Use of Retained Data and Copyright Law in Germany – the German Data Protection Problem to Fight Internet Piracy' (2010) 32 EIPR 174

Deane C, 'Jurisdiction and Online Publishing' (2002) 8 Comms L 237

Cruquenaire A, 'La loi applicable au droit d'auteur: état de la question et perspectives' (2000) 3 Auteurs & Média 210

de Souza L and Waelde C, 'Moral Rights and the Internet: Squaring the Circle' (2002) 3 IPQ 265

Debois H, 'Le droit d'auteur des étrangers en France' (1960) 28 RIDA 79

Demuth T and Rieke A, 'Anonym im World Wide Web' (1998) 11 DuD 623

Díaz C, Claessens J and Preneel B, 'APES: Anonymity and Privacy in Electronic Services' (2003) 27 DuD 143

Dick K, 'Digital Britain – A summary' (2009) 20 Ent LR 283

Dickman JM, 'Anonymity and the Demands of Civil Procedure in Music Downloading Lawsuits' (2008) 82 TLR 1049

Dinwoodie GB, Dreyfuss RC and Kur A, 'The Law Applicable to Secondary Liability in Intellectual Property Cases' (2010) 42 NYU Journal of International Law and Politics 201

Earnshaw C and Jadav S, 'E-Mail Tracing' (2004) 15 C & L 7

Evans MD, 'Protection of Data on the Internet' (2002) 1 IPQ 50

Fauvarque-Cosson B, 'Comparative Law and Conflict of Laws: Allies or Enemies? New Perspectives on an Old Couple' (2001) 49 AJCL 407

Fawcett J, 'The Interrelationships of Jurisdiction and Choice of Law in Private International Law' (1991) 44 Current Legal Problems 39

Fung WMJ and Lakhani A, 'Combatting peer-to-peer file sharing of copyrighted material via anti-piracy laws: issues, trends and solutions' (2013) 29 Computer Law & Security Review 382

Garnett R, 'The Hague Choice of Court Convention: Magnum Opus or Much Ado about Nothing?' (2009) 5 JourPIL 161

Gaubiac Y, 'La Convention de Berne, encore méconnue: commentaire de la décision TGI Paris, 3e ch., sect. B, 20 mai 2008, Sté des arts visuels et de l'image fixe [SAIF] c/SARL Google France, Sté Google Inc' (2008) 11 Communication Commerce Electronique 12

Geist MA, 'Is There a There There? Towards Greater Certainty For Internet Jurisdiction' (2001) 16 Berkeley TechLJ 1345

Geist M, 'Cyberlaw 2.0' (2003) 44 BCL Rev 323

Geller PE, 'Conflicts of Laws in Cyberspace: Rethinking International Copyright in a Digitally Networked World' (1996) 20 Colum VLA JLA 571

Geller PE, 'Conflicts of Laws in Copyright Cases: Infringement and Ownership Issues' (2004) 51 J Copyright Soc'y USA 315

Gillies LE, 'Addressing the "Cyberspace Fallacy": Targeting the Jurisdiction of an Electronic Consumer Contract' (2008) 16 Int J Law Info Tech 242

Ginsburg JC, 'L'exploitation internationale de l'oeuvre audiovisuelle: France/États Unis' (1994) 4 La Semaine Juridique 49, Doctrine 3734

Ginsburg JC, 'Putting Cars on the Information Superhighway: Authors, Exploiters and Copyright in Cyberspace' (1995) 95 Colum L Rev 1466

Ginsburg JC, 'Comment, Extraterritoriality and Multiterritoriality in Copyright Infringement' (1997) 37 Va J Int'l L 587

Ginsburg JC, 'The Cyberian Captivity of Copyright: Territoriality and Authors' Rights in a Networked World' (1999) 15 Santa Clara Comp & Tech LJ 347

Ginsburg JC, 'Copyright Use and Excuse on the Internet' (2000) 24 Colum VLA JLA 1

Ginsburg JC, 'International Copyright: From a "Bundle" of National Copyright Laws to a Supranational Code?' (2000) 47 J Copyright Soc'y USA 265

Ginsburg JC, 'Berne Without Borders: Geographic Indiscretion and Digital Communications' (2002) 2 IPQ 111, 116

Goldsmith JL and Sykes AO, 'The Internet and the Dormant Commerce Clause' (2001) 110 Yale LJ 785

Gutierrez HE, 'Peering Through the Cloud: The Future of Intellectual Property and Computing' (2011) 20 Fed Cir B J 589

Haouideg H, 'Droit d'auteur et droit international prive en belgique' (2006) 207 RIDA 98

Hartley TC, 'The Hague Choice-of-Court Convention' (2006) 31 ELR 414

Hirst M, 'Cyberobscenity and the Ambit of English Criminal Law' (2002) 13 CL 25

Hörnle J, 'The UK Perspective on the Country of Origin Rule in the E-commerce Directive—A Rule of Administrative Law Applicable to Private Law Disputes?' (2004) 12 Int J Law Info Tech 333

Hoeren T, 'IPR und EDV-recht. Kollisionsrechtliche Anknüpfungen bei internationalen EDV-Verträgen' (1993) 3 CR 129

Hoey A, 'Techno-cops: information technology and law enforcement' Int J Law Info Tech 69

Hugenholtz B, 'Why the Copyright Directive is Unimportant, and Possibly Invalid' (2000) 22 EIPR 499

Huniar K, 'The Enforcement Directive – its effects on UK Law' (2006) 28 EIPR 92

Hyland M, 'Copyright, Technology, and Proportionality' (2014) Law Society Gazette 58

Hyland M, 'The Football Association Premier League ruling – the Bosman of exclusive broadcasting rights?' (2012) 17 Comms L 7

Hyland M, 'The seductive interface between adult entertainment and Norwich Pharmacal relief - Golden Eye (International) Ltd v Telefonica UK Ltd [2012] EWHC 723 (Ch) and [2012] EWCA Civ 1740' (2013) 18 *Comms L* 56

Hyland M, 'TV Broadcasters' IP rights bolstered by recent CJEU preliminary ruling' (2013) *Law Society Gazette* 58

Jackson M and Shelly M, 'Black Hats and White Hats: Authorisation of Copyright Infringement in Australia and the United States' (2006) 14 Int J Law Info Tech 28

Jiang M, 'Authoritarian Informationalism: China's Approach to Internet Sovereignty' (2010) 30 SAIS Review 71

Kaplan LGC and Bankoff JR, 'Of Satellites and Copyright: Problems of Overspill and Choice of Law' (1993) 7 Emory Int'l L Rev 727

Kern P, 'The EC "Common Position" on Copyright Applicable to Satellite and Cable' (1993) 8 EIPR 276

King KF, 'Geolocation and Federalism on the Internet: Cutting Internet Gambling's Gordian Knot' (2010) 11 Colum Sci & Tech L Rev 41

King KF, 'Personal Jurisdiction, Internet Commerce, and Privacy: the Pervasive Legal Consequences of Modern Geolocation Technologies' (2011) 21 Alb LJ Sci & Tech 61

Kleinschmidt B, 'An International Comparison of ISP's Liabilities for Unlawful Third Party Content' (2010) 18 Int J Law Info Tech 332

Koempel F, 'Digital Economy Bill' (2010) 16 CTRLR 39

Kohl U, 'The Rule of Law, Jurisdiction and the Internet' (2004) 12 Int J Law Info Tech 365

Koumantos G, 'Sur le droit international privé du droit d auteur' (1979) Il Diritto di Autore 616

Koumantos G, 'Privat International Law and the Berne Convention' (1988) 24 Copyright 415

Kuner C, 'Data Protection Law and International Jurisdiction on the Internet (Part 1)' (2010) 18 Int J Law Info Tech 176

Kuner C, 'Data Protection Law and International Jurisdiction on the Internet (Part 2)' (2010) 18 Int J Law Info Tech 227

Kur A, 'Applicable Law: An Alternative Proposal for International Regulation – The Max-Planck Project on International Jurisdiction and Choice of Law' (2005) 30 Brook J Int L 951

Lanois P, 'Caught in the Clouds: The Web 2.0, Cloud Computing, and Privacy?' (2010) 9 Northwestern Journal of Technology and Intellectual Property 29

Lee JCJ, 'The ongoing design duty in Universal Music Australia Pty Ltd v Sharman License Holdings Ltd – Casting the scope of copyright infringement even wider' (2007) 15 Int J Law Info Tech 275

Leong SHS, 'Pre-Action Discovery against a Network Service Provider and Unmasking the John Does of Alleged Online Copyright Infringements in Singapore' (2009) 31 EIPR 185

Leong SHS and Saw CL, 'Copyright Infringement in a Borderless World – Does Territoriality Matter? Society of Composers, Authors and Music Publishers of Canada v Canadian Association of Internet Providers [2004] 2 SCR 427' (2007) 15 Int J Law Info Tech 38

Liebman K, 'Opinion: Untying the Knot — Copyright Law and the New Technologies' (1993) 1 Int J Law Info Tech 225

Lloyd IJ, 'Liabilities for the Contents of On-line Services' (1995) 3 Int J Law Info Tech 273

Lloyd IJ, 'Shopping in Cyberspace' (1993) 1 Int J Law Info Tech 335

Lloyd I, Kierkegaard S, Waters N, Greenleaf G, Bygrave LA and Saxby S, '30 Years On – The Review of the Council of Europe Data Protection Convention 108' (2011) 27 CLS Rev 223

Lundevall-Unger P and Tranvik T, 'IP Addresses – Just a Number?' (2011) 19 Int J Law Info Tech 53

Lundstedt L, 'Jurisdiction and the Principle of Territoriality in Intellectual Property Law: Has the Pendulum Swung Too Far in the Other Direction?' (2001) 32 IIC 124

Maier B, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 Int J Law Info Tech 142

Frederick A Mann, 'The Doctrine of Jurisdiction in International Law' (1964) 111 Recueil des Cours 1

Manolopoulos A, 'Raising "Cyber-Borders": The Interaction Between Law and Technology' (2003) 11 Int J Law Info Tech 40

Mason S and George E, 'Digital Evidence and "Cloud" Computing' (2011) 27 CLS Rev 524

Melzer MA, 'Copyright Enforcement in the Cloud' (2010-2011) 21 Fordham Intell Prop Media & Ent L J 403

Mo YJ, 'Case commentary: Cinepoly Records Co Ltd & Others v Hong Kong Broadband Network Ltd & Others' (2009) 31 EIPR 48

Morcom C, 'Trade marks and the Internet: Where Are We Now?' (2012) 34 EIPR 40

Morrison A and Gillies LE, 'Securing Webcast Content in the European Union: Copyright, Technical Protection and Problems of Jurisdiction on the Internet' (2002) 24 EIPR 74

Morris, PS, 'Pirates of the Internet, At Intellectual Property's End With Torrents and Challenges for Choice of Law' (2009) 17 Int J Law Info Tech 282

Nanda VP, 'The Landmark 2005 Hague Convention on Choice of Court Agreements' (2007) 42 Texas Intl LJ 773

Nissan E, 'Legal Evidence, Police Intelligence, Crime Analysis or Detection, Forensic Testing, and Argumentation: An Overview of Computer Tools or Techniques' (2009) 17 Int J Law Info Tech 1

North P, 'Private International Law: Change or Decay?' (2001) 50 ICLQ 447

Plenter S, 'Choice of Law Rules for Copyright Infringements in the Global Information Infrastructure: A Never-Ending Story' (2003) 23 EIPR 313

Rashid AA, 'The Hague Convention on Choice of Court Agreements 2005: An Overview' (2005) 45 Indian JIntl L 558

Redfern P, 'Precise Identification through a Multi-purpose Personal Number Protects Privacy' (1993) 1 Int J Law Info Tech 305

Reiter MK and Rubin AD, 'Crowds: Anonymity for Web Transactions' (1998) 1 ACM Transactions on Information and System Security

Rose D and O' Sullivan N, 'Football Dataco v Yahoo! Implications of the ECJ judgment' (2012) 7 Journal of Intellectual Property Law & Practice 792

Rotstein F, 'Is there an international intellectual property system? Is there an agreement between states as to what the objectives of intellectual property should be?' (2011) 33 EIPR 1

Rubenstein I, Lee R and Schwartz PM, 'Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches' (2008) 75 UCLR 261

Rubin H, Fraser L, and Smith M, 'US and International Law Aspects of the Internet: Fitting Square Pegs Into Round Holes' (1995) 3 Int J Law Info Tech 117

Saraf B and Kazi AUS, 'Analysing the application of Brussels I in regulating e-commerce jurisdiction in the European Union – Success, deficiencies and proposed changes' (2013) 29 Computer Law & Security Review 127

Schønning P, 'Licensing Authors' Rights on the Internet' (2000) 31 IIC 967

Schulz A, 'The Hague Convention of 30 June 2005 on Choice of Court Agreements' (2006) 2 JourPIL 243

Smartt U, *Media and Entertainment Law* (1st edn, Routledge 2011)

Snail S, 'Cyber crime in South Africa – Hacking, cracking, and other unlawful online activities' (2009) 1 JILT 1

Stokes S, 'Intellectual Property and Technology Issues' (2010) 79 COB 1

Svantesson DJB, 'A legal method for solving issues of Internet regulation' (2011) 19 Int J Law Info Tech 243

Svantesson DJB, 'E-Commerce Tax: How the Taxman Brought Geography to the "Borderless" Internet' (2007) 11 Revenue LJ 1

Svantesson DJB, 'Geo-Location Technologies and other Means of Placing Borders on the "Borderless" Internet' (2004) 23 J Marshall J Computer & Info L 101

Svantesson DJB, 'Jurisdictional Issues in Cyberspace; At the Crossroads - the Proposed Hague Convention and the Future of Internet Defamation' (2002) 18 CLSR 191

Svantesson DJB and Clarke R, 'Privacy and Consumer Risks in Cloud Computing' (2010) 26 CLS Rev 391

Svantesson DJB, 'The characteristics making Internet communication challenge traditional models of regulation – What every international jurist should know about the Internet' (2005) 13 Int J Law Info Tech 39

Svantesson DJB, 'Time for the Law to take Internet Geolocation Technologies Seriously' (2012) 8 Journal of Private International Law 473

Tang ZS, 'Private International Law in Consumer Contracts: A European Perspective' (2010) 6 Journal of Private International Law 225

Tapper C, 'Evanescent Evidence' (1993) 1 Int J Law Info Tech 35

Tapper C, 'Reform of the Law of Evidence in Relation to the Output from Computers' (1995) 3 Int J Law Info Tech 79

Taylor M, Haggerty J, Gresty D and Berry T, 'Digital Evidence from peer-to-peer networks' (2011) 27 Computer Law & Security Review 647

Thum D and Bettinger T, 'Territorial Trademark Rights in the Global Village – International Jurisdiction, Choice of Law and Substantive Law for Trademark disputes on the Internet: Part 1' (2000) 31 IIC 162

Torremans P, 'Licences and Assignments of Intellectual Property Rights under the Rome I Regulation' (2008) 4 Jour PIL 397

Trimble M, 'The Future of Cybertravel: Legal Implications of the Evasion of Geolocation' (2012) 22 Fordham Intell Prop Media & Ent LJ 567

van Dellen M, 'Anonymity on the Internet. What does the Concept of Anonymity Mean?' (2002) 9 EDI LR 1

Vamialis A, 'Online defamation: confronting anonymity' (2013) 21 Int J Law Info Tech 31

Vaver D, 'Recent Copyright Law Developments Reform?' (2010) 22 IPJ 1

Vincentis OB, 'When Rights Clash Online: The Tracking of P2p Copyright Infringements Vs. the EC Personal Data Directive' (2008) 16 Int J Law Info Tech 270

Vinje TC, 'Should We Begin Digging Copyright's Grave?' (2000) 22 EIPR 551

Vlas P (ed), 'Dutch Private International Law: The 2001 Act regarding Conflict of Laws on Torts' (2003) 50 NILR 221

Wadlow C, 'Intellectual Property and the Rome Contracts Convention' (1997) 1 EIPR 11

Walden I, 'Forensic Investigations in Cyberspace for Civil Proceedings' (2004) 18 Int'l Rev L Computers Tech 275

Withers C, 'Jurisdiction and Applicable Law in Antitrust Tort Claims' (2002) 6 JBL 250

Wong MWS, 'Cyber-trespass and "Unauthorized Access" as Legal Mechanisms of Access Control: Lessons from the US Experience' (2007) 15 Int J Law Info Tech 90

Zekos GI, 'State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction' (2007) 15 Int J Law Info Tech 1

ONLINE JOURNALS

Lloyd I, 'Privacy, Anonymity and the Internet' (2009) 13 EJCL
<<http://www.ejcl.org/131/art131-3.pdf>> accessed 6 May 2014

Koumartzis N and Veglis A, 'Internet regulation: The need for more transparent internet filtering systems and improved measurement of public opinion on internet filtering' (2011) 16 First Monday

<<http://firstmonday.org/ojs/index.php/fm/article/view/3266/3071>> accessed 14 May 2014

UK COMMITTEE REPORTS, CONSULTATIONS, NOTES, GUIDANCE

European Union Committee, *The Rome II Regulation* (HL 2003-04, 66)

Home Office, 'Consultation: Transposition of Directive 2006/24/EC' (12 August 2008)

<<http://www.homeoffice.gov.uk/documents/cons-2008-transposition?view=Binary>> accessed 23 November 2008

Information Commissioner's Office (ICO), 'Good Practice Note - Collecting personal information using websites' (3 June 2007)

<http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/collecting_personal_information_from_websites_v1.0.pdf> accessed 30 June 2010

Joint Committee on Human Rights, *Draft Voluntary Code of Practice on Retention of Communications Data under Part 11 of the Anti-terrorism, Crime and Security Act 2001* (2002-03, HL 181, HC 1272)

Ministry of Justice, *Defamation and the internet: the multiple publication rule* (CP/20/09, 16 September 2009)

<<https://www.justice.gov.uk/consultations/docs/defamation-consultation-paper.pdf>> accessed 9 July 2012

Ministry of Justice, 'Guidance on the Law Applicable to Contractual Obligations (Rome I) – Outline of the Main Provisions' (February 2010)

<<http://www.justice.gov.uk/publications/docs/guidance-law-contractual-obligations-romei.pdf>> accessed 24 February 2010

Vollmer PM, *Defamation* (House of Lords Library Note, LLN 2010/016, 5 July 2010)

OFFICIAL DOCUMENTS PUBLISHED BY INTERNATIONAL ORGANISATIONS AND GOVERNMENT DEPARTMENTS

American Law Institute, *Intellectual Property: Principles Governing Jurisdiction, Choice of Law, and Judgments in Transnational Disputes* (WIPO, 2008)
<<http://www.wipo.int/wipolex/en/details.jsp?id=7687>> accessed 13 July 2012

Article 29 Data Protection Working Party, 'Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data' (11818/02/EN/Final, WP 64, 11 October 2002)
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp64_en.pdf> accessed 7 July 2012

Article 29 Data Protection Working Party, 'Opinion 9/2004 on a Draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism' 4 et seq (11885/04/EN, WP 99, 9 November 2004)
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp99_en.pdf> accessed 6 July 2012

Article 29 Data Protection Working Party, 'Opinion 4/2007 on the concept of personal data' (1248/07/EN, WP 136, 20 June 2007)
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> accessed 6 July 2012

Article 29 Data Protection Working Party, 'Report 01/2010 on the second joint enforcement action: Compliance at national level of Telecom Providers and ISPs with the obligations required from national traffic data retention legislation on the legal basis of articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC amending the e-Privacy Directive' 19 (68/10/EN, WP 172, 13 July 2010)
<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp172_en.pdf> accessed 7 July 2012

Austin G, 'Private International Law and Intellectual Property Rights - A Common Law Overview' (WIPO Forum on Private International Law and Intellectual Property, WIPO/PIL/01/5, 2001)

Díaz C and Preneel B, 'Anonymous Communication' (SICS workshop WHOLES – A Multiple View of Individual Privacy in a Networked World, Stockholm January 2004)

Dreyfuss RC and Ginsburg JC, 'Draft Convention on Jurisdiction and Recognition of Judgments in Intellectual Property Matters' (WIPO Forum on Private International Law and Intellectual Property, WIPO/PIL/01/7, 2001)

Ginsburg JC, 'Private International Law Aspects of the Protection of Works and Objects of Related Rights Transmitted Through Digital Networks' (WIPO Forum on Private International Law and Intellectual Property, GCPIC/2, 1998)

Ginsburg JC and Lucas A, 'The Role of Private International Law and Alternative Dispute Resolution in WIPO, Intellectual Property on the Internet: A Survey of Issues' (WIPO/INT/02, 2002)

Harms L, 'The Enforcement of Intellectual Property Rights By Means of Criminal Sanctions: An Assessment' (WIPO Advisory Committee on Enforcement, WIPO/ACE/4/3, 7 September 2007)

Hartley T and Dogauchi M, Explanatory Report on the Convention of 30 June 2005 on Choice of Court Agreements (*HCCH*, 2007) <<http://www.hcch.net/upload/expl37e.pdf>> accessed 18 August 2012

HM Government, European E-Commerce Taskforce, 'Empowered Consumers, Unleashed Business' (August 2013) <<http://dpalliance.org.uk/wp-content/uploads/2013/09/EU-e-commerce-taskforce-FINAL-REPORT.pdf>> accessed 7 April 2014

ICO, 'Information Commissioner's Office: initial analysis of the European Commission's proposals for a revised data protection legislative framework' (V1.0, 27

February 2012)

<http://ico.org.uk/news/current_topics/~media/documents/library/Data_Protection/Research_and_reports/ico_initial_analysis_of_revised_eu_dp_legislative_proposals.ashx> accessed 10 May 2014

Lucas A, 'Private International Law Aspects of the Protection of Works and of the Subject Matters of Related Rights Transmitted over Digital Networks' (WIPO Forum on Private International Law and Intellectual Property, WIPO/PIL/01/1 Prov, 2000)

Office of the Leader of the House of Commons, *The Government's Draft Legislative Programme* (Cm 7372, 2008)

Strassman PA, 'Risk-Free Access into the Global Information Infrastructure via Anonymous Re-mailers' (Symposium on the Global Information Infrastructure: Information, Policy & International Infrastructure, Cambridge, MA, 28-30 January 1996) <<http://www.strassmann.com/pubs/anon-remail.html>> accessed 5 June 2014

TERA Consultants, 'Building a Digital Economy: The Importance of Saving Jobs in the EU's Creative Industries' (*International Chamber of Commerce/BASCAP*, March 2010) <<http://www.droit-technologie.org/upload/dossier/doc/219-1.pdf>> accessed 16 April 2014

WIPO, 'Agreed Statements concerning the WIPO Copyright Treaty adopted by the Diplomatic Conference on December 20, 1996' <http://www.wipo.int/treaties/en/text.jsp?file_id=295456> accessed 26 May 2014

WIPO, 'Joint Recommendation Concerning Provisions on the Protection of Marks, and other Industrial Property Rights in Signs, on the Internet' (845(E), 24 September-3 October 2001) <<http://www.wipo.int/export/sites/www/freepublications/en/marks/845/pub845.pdf>> accessed 9 May 2014

ACADEMIC REPORTS/REPORTS WRITTEN BY ACADEMIC BODIES

Bently L, Derclaye E, Dinwoodie GB, Dreier T, Dusollier S, Geiger C, Griffiths J, Hilty R, Hugenholtz PB, Janssens M-C, Kretschmer M, Metzger A, Peukert A, Ricolfi M, Senftleben M, Strowel A, Vivant M, Xalabarder R, 'Opinion on The Reference to the CJEU in Case C-466/12 *Svensson*' (*European Copyright Society*, 15 February 2013) <http://www.ivir.nl/news/European_Copyright_Society_Opinion_on_Svensson.pdf> accessed 31 May 2014

de Win B, Naessens V, Díaz C, Seys S, Goemans C, Claessens J, de Decker B, Dumortier J and Preneel B, 'APES Deliverable 3 - Technologies overview' (*COSIC*, 12 November 2001) <<http://www.cosic.esat.kuleuven.be/publications/article-108.pdf>> accessed 18 August 2012

Díaz C, Naessens V, Claessens J, de Win B, Seys S, de Decker B and Preneel B, 'APES Deliverable D5: Tools for Technologies and Applications' (*COSIC*, 19 November 2002) <<https://www.cosic.esat.kuleuven.be/publications/article-107.pdf>> accessed 18 August 2012

Claessens J, Díaz C, Nikova S, Naessens V, de Win B, Goemans C, Seys S, Loncke M, Dumortier J, de Decker B and Preneel B, 'APES Deliverable 7 - Applications Requirements for Controlled Anonymity' (*COSIC*, May 2003) <<http://www.cosic.esat.kuleuven.be/publications/article-106.pdf>> accessed 18 August 2012.

Dumortier J, Loncke M, Goemans C, 'APES Deliverable 4 - General Report of the Legal Issues' (*COSIC*, March 2003) <https://www.cosic.esat.kuleuven.be/apes/docs/APES_d4.doc.gz> accessed 18 August 2012

European Max Planck Group, Principles for Conflict of Laws in Intellectual Property, The Draft (*Max-Planck-Gesellschaft*, 25 March 2011) <<http://www.cl-ip.eu/files/pdf2/draft-clip-principles-25-03-20117.pdf>> accessed 12 July 2012

Hess B, Pfeiffer T and Schlosser P, 'Report on the Application of Brussels I Regulation in the Member States, Study JLS/C4/2005/03' (*Ruprecht-Karls-Universität Heidelberg, Institut für ausländisches und internationales Privat- und Wirtschaftsrecht*, September

2007) <http://ec.europa.eu/civiljustice/news/docs/study_application_brussels_1_en.pdf>
accessed 2 April 2014

Hugenholtz B, 'Copyright without Frontiers: is there a future for the Satellite and Cable Directive' (*IViR*, 2005)

<<http://www.ivir.nl/publications/hugenholtz/copyrightwithoutfrontiers.pdf>> accessed 13 June 2014

Kim H and Dobson S, 'An improved approach to geographically locating web clients' (*Department of Computer Science, Trinity College Dublin*)

<http://www.academia.edu/2885294/An_improved_approach_to_geographically_locating_web_clients> accessed 10 May 2014

Max Planck Institute for Comparative and International Private Law Hamburg, 'Working Group on Questions of Jurisdiction and Choice of Law in Intellectual Property Matters' (8 June 2010)

<http://www.mpipriv.de/ww/en/pub/research/research/research_work/international_private_law_proc/commercial_and_competition_law/workgroup_intellectual_propert.cfm>
accessed 13 July 2012

Seys S, Díaz C, de Win B, Naessens V, Goemans C, Claessens J, Moreau W, de Decker B, Dumortier J and Preneel B, 'APES Deliverable 2 - Requirement study of different applications (*COSIC*, 11 May 2001)

<<http://www.cosic.esat.kuleuven.be/publications/article-450.pdf>> accessed 19 August 2012

SUNDRY OTHER REPORTS AND RESEARCH PAPERS

ALAI, 'Report and Opinion on the making available and communication to the public in the internet environment – focus on linking techniques on the Internet' (16 September 2013) <<http://www.alai.org/assets/files/resolutions/making-available-right-report-opinion.pdf>> accessed 7 May 2014

BPI, 'Digital Music Nation 2013 – The UK's digital music landscape' (January 2013)
<https://www.bpi.co.uk/assets/files/BPI_Digital_Music_Nation_2013.PDF> accessed 8
May 2014

BPI, 'Digital Music Nation 2010 – The UK's legal and illegal digital music landscape'
(December 2010)
<<http://www.bpi.co.uk/assets/files/Digital%20Music%20Nation%202010.pdf>>
accessed 16 July 2012

Kay D, 'Online Copyright Infringement Tracker Annex 1 – Individual content types
Wave 3 (Covering period Nov 12-Jan 13)' (*Kantar Media*, 2013)
<<http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/w3/wave3.pdf>> accessed 8 May 2014

Kay D, 'Online Copyright Infringement Tracker Wave 3 (Covering period Nov 12-Jan
13) Overview and key findings' (*Kantar Media*, 2013)
<<http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/w3/annexw3.pdf>> accessed 8 May 2014

Edwards S, Kamina P and Pfeifer KN, 'Modern copyright for digital media. Legal
analysis and EBU proposals' (*EBU*, March 2012) <http://www.ebu.ch/regis-tration/policy2010/images/EBU%20Copyright%20WHITE%20Paper_EN_FINAL.pdf>
accessed 2 July 2012

Financial Markets Committee, 'Legal assessment of the conversion of the Rome
Convention to a Community instrument' (April 2006)
<www.fmlc.org/Documents/April06Issue121.pdf> accessed 1 July 2012

Hargreaves I, 'Digital Opportunities – A Review of Intellectual Property and Growth'
(May 2011) <<http://www.ipo.gov.uk/ipreview-finalreport.pdf>> accessed 24 June 2012

IFPI, 'IFPI Digital Music Report 2013 – Engine of a digital World' (2013)
<<http://www.ifpi.org/content/library/DMR2013.pdf>> accessed 16 April 2014

IFPI, 'IFPI Digital Music Report

2014 – Lighting up New Markets’ (April 2014)
<<http://www.ifpi.org/downloads/Digital-Music-Report-2014.pdf>> accessed 8 May 2014

IFPI, ‘IFPI Digital Music Report
2011 – Music at the touch of a button’ (20 January 2012)
<<http://www.ifpi.org/content/library/DMR2011.pdf>> accessed 16 July 2012

Internet World Stats, ‘United States of America – Internet Usage and Broadband Usage
Report’ (November 2009) <<http://www.internetworldstats.com/top25.htm>> accessed 12
August 2012

Internet World Stats, ‘Internet Usage in Europe’ (30 June 2012)
<<http://www.internetworldstats.com/stats4.htm>> accessed 16 April 2014

Latapy M, Clémence Magnien and Raphaël Fournier, ‘Technical Report on
Quantification of Paedophile Activity in a Large P2P System’ (2009) 7
<<http://antipaedo.lip6.fr/T24/TR/quantification.pdf>> accessed 4 July 2012

Michaels R, ‘The Functional Method of Comparative Law’ (*Duke Law School Legal
Studies*, Research Paper 87, November 2005)
<http://lsr.nellco.org/cgi/viewcontent.cgi?article=1025&context=duke_fs> accessed 9
May 2014

Ofcom, ‘Online Infringement of Copyright and the Digital Economy Act 2010 Draft
Initial Obligations Code’ (28 May 2010)
<[http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-
infringement/summary/condoc.pdf](http://stakeholders.ofcom.org.uk/binaries/consultations/copyright-infringement/summary/condoc.pdf)> accessed 13 August 2012

Ofcom, ‘“Site Blocking” to reduce online copyright infringement, A review of sections
17 and 18 of the Digital Economy Act’ (27 May 2010)
<<http://stakeholders.ofcom.org.uk/binaries/internet/site-blocking.pdf>> accessed 8 May
2014

Peukert A, 'Territoriality and Extraterritoriality in Intellectual Property Law' (*SSRN*, 19 April 2010) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1592263> accessed 31 May 2014

THESIS

van Eechoud M, 'Choice of Law in Copyright and Related Rights. Alternatives to the Lex Protectionis' (DPhil thesis, University of Amsterdam 2003)

NEWSPAPER/MAGAZINE ARTICLES

Akst D, 'Postcard from Cyberspace: The Cutting Edge, The Helsinki Incident and the Right to Anonymity' *LA Times* (Los Angeles, 22 February 1995)

Burton T, 'US industry group white paper says geolocation technologies are not precise enough to identify taxing jurisdiction reliably, rendering EU VAT rules unworkable' (*THE*, 29 October 2002)

<<http://www.timeshighereducation.co.uk/story.asp?storyCode=172460§ioncode=26>> accessed 30 June 2010

Carolan M, 'Legal action to stop UPC users downloading illegally' (*The Irish Times*, 10 February 2014) <<http://www.irishtimes.com/news/crime-and-law/courts/legal-action-to-stop-upc-users-downloading-illegally-1.1686474>> accessed 8 May 2014

'Geography and the net – Putting it in its place' *The Economist* (9 August 2001) 18

'I have a stream – The land of Abba takes to streaming' (*The Economist*, 22 March 2014) <<http://www.economist.com/news/business/21599353-land-abba-takes-streaming-i-have-stream>> accessed 21 May 2014

'Imitation v Inspiration' *The Economist* (US, 14 September 2002) 11

Kuchler H, 'UK "leads the world" in e-commerce' (*Financial Times*, 19 March 2012)
<<http://www.ft.com/cms/s/0/ef3e1a04-71b4-11e1-8497-00144feab49a.html#axzz2yDydFfej>> accessed 7 April 2014

Orpaz I, 'Russian Internet giant Yandex acquiring Israeli geolocation startup Kitlocate' (*Haaretz*, 18 March 2014) <<http://www.haaretz.com/business/.premium-1.580480>> accessed 21 May 2014

Sherwin A, 'Music sales fail to go in One Direction as growth turns to 3.9% decrease' (*The Independent*, 18 March 2014) <<http://www.independent.co.uk/arts-entertainment/music/news/music-sales-fail-to-go-in-one-direction-as-growth-turns-to-39-decrease-9200304.html>> accessed 21 May 2014

Steiner P, 'On the Internet, nobody knows you're a dog' (1993) 69 *The New Yorker* 61

'The Great Firewall, The Art of Concealment' (*The Economist*, 6 April 2013)
<<http://www.economist.com/news/special-report/21574631-chinese-screening-online-material-abroad-becoming-ever-more-sophisticated>> accessed 14 May 2014

White A, 'IP Addresses Are Personal Data, E.U. Regulator Says' (*The Washington Post*, 22 January 2008) <<http://www.washingtonpost.com/wp-dyn/content/article/2008/01/21/AR2008012101340.html>> accessed 30 June 2010

WEBSITES

Akamai, 'EdgeScape' (*Akamai Technologies*, 2012)
<<http://akamai.com/html/technology/products/edgescape.html>> accessed 13 August 2012

Anonymizer 'How it Works' (*Anonymizer*, 2012)

<<http://www.anonymizer.com/homeuser/universal#features>> accessed 3 July 2012

APNIC, 'About APNIC' <www.apnic.net/about-APNIC/organization> accessed 14 August 2012

ARIN, 'ARIN at a glance' <www.arin.net/about_us/overview.html> accessed 14 August 2012

BBC, 'Judge rules three were defamed on Facebook' (*BBC News Northern Ireland*, 6 February 2013) <<http://www.bbc.co.uk/news/uk-northern-ireland-21354945>> accessed 8 April 2014

BBC, 'BitTorrent study finds most file-sharers are monitored' (*BBC News Technology*, 4 September 2012) <<http://www.bbc.co.uk/news/technology-19474829>> accessed 24 May 2014

BBC, 'UK Piracy warning letters delayed until 2015' (*BBC News Technology*, 6 June 2013) <<http://www.bbc.co.uk/news/technology-22796723>> accessed 8 May 2014

Bérard L, 'Intellectual Property Rights Protection on the Internet in France: The End of Hadopi?' (*LSE*, 29 January 2014)

<<http://blogs.lse.ac.uk/mediapolicyproject/2014/01/29/intellectual-property-rights-protection-on-the-internet-in-france-the-end-of-hadopi>> accessed 3 June 2014

Byrt S and Hart D, 'Copyright Across Borders' in Mayer Brown, 'Expert Guide: Intellectual Property' (*Corporate Live Wire*, December 2011)

<http://www.mayerbrown.com/files/News/766c77f9-5f13-478c-aec1-17ecc831941e/Presentation/NewsAttachment/59ac67c0-42c9-458d-9fad-1bbca7f87dda/ART_BYRT_HART_DEC11_COPYRIGHT-ACCROSS-BORDERS.PDF> accessed 23 August 2012

Caida, 'CAIDA's Geolocation Tools Comparison' (*Caida*, 6 September 2009) <<http://caida.org/projects/cybersecurity/geolocation/>> accessed 6 July 2012

Center for High Assurance Computer Systems, 'Onion Routing' <www.onion-router.net> accessed 3 July 2012

Canadian Centre for Child Protection Inc, 'Cleanfeed Canada' (*cybertip!ca*) <<https://www.cybertip.ca/app/en/projects-cleanfeed>> accessed 14 May 2014

Council of Europe, 'Convention on Cybercrime – Status as of: 14/8/2012' <<http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG>> accessed 14 August 2012

Davis W, 'Court Rules Web Users Have Expectation of Privacy' (*MediaPost*, 24 April 2008) <http://www.mediapost.com/publications/?fa=Articles.showArticle&art_aid=81306> accessed 1 July 2010

Department for Culture, Media & Sport, 'Next steps to tackle internet piracy' (26 June 2012) <<https://www.gov.uk/government/news/next-steps-to-tackle-internet-piracy>> accessed 3 June 2014

Digital Element, 'Geolocation Technology' (*Digital Envoy*, 2012) <<http://www.digitalelement.com>> accessed 6 July 2012

Digital Envoy, 'Digital Envoy Alliance with Melbourne IT gives global boost to innovative internet marketing and eCommerce technology; hoping to avoid "Cookies" controversy, Australian firm embraces NetAcuity as the emerging standard for non-invasive web tracking and customer service activities' (9 April 2000) <http://www.digitalenvoy.net/news/press_releases/2000/pr_040900.html> accessed 14 August 2012

DocoDoco, 'The beginning of online distribution of videos – Management of regional distribution by ways of IP Geolocation' <<http://www.docodoco.jp/en/block/column01.html>> accessed 14 April 2014

Ecommerce Technology, 'Push-Pull Technology'

<<http://ecommercetechnology.org/english/data/70.htm>> accessed 3 June 2014

Edelman B, 'Shortcomings and Challenges in the Restriction of Internet Retransmissions of Over-the-air Television content to Canadian Internet Users' <http://cyber.law.harvard.edu/archived_content/people/edelman/pubs/jump-091701.pdf> accessed 29 June 2010

EPIC, 'Children's Online Privacy Protection Act (COPPA)' <<http://epic.org/privacy/kids/>> accessed 3 July 2010

European Council, 'EU unitary patent – a historic breakthrough' (*European Council*, 29 June 2012) <<http://www.european-council.europa.eu/home-page/highlights/eu-unitary-patent-%E2%80%93-a-historical-breakthrough?lang=en>> accessed 2 July 2012

European Parliament Press Service, 'European Parliament rejects ACTA' (*European Parliament News*, 4 July 2012) <<http://www.europarl.europa.eu/news/en/pressroom/content/20120703IPR48247/html/European-Parliament-rejects-ACTA>> accessed 16 August 2012

Gasaway L, 'Criminal copyright infringement' (*Copyright Corner*, April 2004) <<http://www.unc.edu/~unclng/copy-corner66.htm>> accessed 16 August 2012

Google, 'IPv6 Statistics' (1 June 2014) <<https://www.google.com/intl/en/ipv6/statistics/html>> accessed 3 June 2014

Gunderson SH (Google), 'Global IPv6 Statistics – Measuring the current state of IPv6 for ordinary users' (RIPE 57, 26-30 October 2008) <http://meetings.ripe.net/ripe-57/presentations/Colitti-Global_IPv6_statistics_-_Measuring_the_current_state_of_IPv6_for_ordinary_users_.7gzD.pdf> accessed 6 July 2012

Gurtner B and Christensen J, 'Beyond Bretton Woods: The Transnational Economy in Search of New Institutions - The Race to the Bottom: Incentives for New Investment?' (*tax justice network*, 15-17 October 2008) <http://www.taxjustice.net/cms/upload/pdf/Bruno-John_0810_Tax_Comp.pdf> accessed 2 July 2012

Hart D, 'Star Wars Episode III – English Supreme Court decision: A New Hope for the enforcement of non-EU copyrights, or a Phantom Menace for UK-domiciled entities?' (*Mayer Brown*, 13 September 2011)

<<http://www.mayerbrown.com/files/Publication/66ac2a8d-59e2-4df4-b9a2-63a0190fd2f2/Presentation/PublicationAttachment/e687d1a6-f0f9-4c52-af8c-795d4509b1ad/11551.pdf>> accessed 23 August 2012

HCCH, 'Members' <http://www.hcch.net/index_en.php?act=states.listing> accessed 16 August 2012

HCCH, '37: Convention of 30 June 2005 on Choice of Court Agreements - Members of the Organisation'

<http://www.hcch.net/index_en.php?act=conventions.statussprint&cid=98> accessed 12 December 2009

Herbert Smith LLP, 'Judicial Review of the Digital Economy Act 2010 upholds online infringement provisions but lets ISPs off the hook on costs' (*Herbert Smith IP newsflash*, 3 May 2011) <[http://www.herbertsmith.com/NR/rdonlyres/21F719F3-5040-42C9-8362-](http://www.herbertsmith.com/NR/rdonlyres/21F719F3-5040-42C9-8362-5D51825C550A/0/20110503JudicialreviewoftheDigitalEconomyActJBSRJMJG.html)

[5D51825C550A/0/20110503JudicialreviewoftheDigitalEconomyActJBSRJMJG.html](http://www.herbertsmith.com/NR/rdonlyres/21F719F3-5040-42C9-8362-5D51825C550A/0/20110503JudicialreviewoftheDigitalEconomyActJBSRJMJG.html)> accessed 6 July 2012

Hollaar LA, 'Chapter 1: An Overview of Copyright' (*Digital Law Online*, 2002) <<http://digital-law-online.info/lpdi1.0/treatise16.html>> accessed 23 July 2010

Hunt A, 'David Cameron wants fresh push on communications data' (*BBC News Politics*, 30 January 2014) <<http://www.bbc.co.uk/news/uk-politics-25969918>> accessed 3 June 2014

Information Technology Association of America (ITAA), 'ECommerce Taxation and the Limitations of Geolocation Tools'

<<http://www.sethf.com/nitke/geolocationpaper.pdf>> accessed 14 August 2012

Jacobus P, 'Building fences, one by one' (*CNET News*, 19 April 2001)

<<http://news.cnet.com/2009-1023-255774-2.html>> accessed 6 July 2012

LACNIC, 'LACNIC Acerca de LACNIC' <lacnic.net/sp/sobre-lacnic/>
accessed 14 August 2012

Landmark Interactive, 'Landmark Interactive in the News' (*Landmark Media Enterprises*, 2010) <http://landmarkinteractive.com/news_releases.php> accessed 6 July 2012

Legalis, 'Cour d'appel de Paris, 13ème chambre, section B, Arrêt du 27 avril 2007' (*LEGALISnet*, 27 April 2007) <http://www.legalis.net/jurisprudence-decision.php3?id_article=1954> accessed 6 July 2012

Legalis, 'Cour d'appel de Paris 13ème chambre, section A, Arrêt du 15 mai 2007' (*LEGALISnet*, 15 May 2007) <http://www.legalis.net/jurisprudence-decision.php3?id_article=1955> accessed 6 July 2012

Lovells H and Shaw A, 'Pirate Bay watch: UK ISPs ordered to block The Pirate Bay' (*ACC*, 20 July 2012) <<http://www.lexology.com/library/detail.aspx?g=29d6e1b2-2c1a-40b8-92f9-0e53a166dd93>> accessed 7 May 2014

Marketwire, 'Quova's Geolocation Data Helps Continental Airlines Improve Web Banner Click-Through Rate by 200 Percent' (24 March 2009)
<<http://www.marketwire.com/press-release/quovas-geolocation-data-helps-continental-airlines-improve-web-banner-click-through-nyse-cal-1237066.htm>> accessed 21 August 2012

Marketwire, 'PricewaterhouseCoopers (PwC) Completes Annual Audit of Quova IP Geolocation Data' (14 April 2009) <<http://www.marketwire.com/press-release/pricewaterhousecoopers-pwc-completes-annual-audit-of-quova-ip-geolocation-data-1233911.htm>> accessed 21 August 2012

McClelland R, 'Attorney-General's Department – Committee Report on Cybercrime Legislation Amendment Bill' (*MMD Newswire*, 19 August 2011)

<<http://www.mmdnewswire.com/committee-report-on-cybercrime-legislation-amendment-bill-60083.html>> accessed 7 July 2012

McIntyre TJ, 'Filter or Else! Music Industry Sues Irish ISP' (*Society for Computers & Law*, 3 April 2008) <<http://www.scl.org/site.aspx?i=ed1049>> accessed 6 July 2012

Neustar, 'IP Geolocation Can Ensure Compliance with New iGaming Regulations' <http://www.neustar.biz/resources/whitepapers/ensure-uigea-compliance-whitepaper#.U030lv1_s3I> accessed 16 April 2014

Neustar[®] IP Intelligence, 'GeoPoint REST API Guide' (2011) <<http://developer.quova.com/docs>> accessed 6 July 2012

Ofcom, 'New measures to protect online copyright and inform consumers' (26 June 2012) <<http://media.ofcom.org.uk/2012/06/26/new-measures-to-protect-online-copyright-and-inform-consumers/>> accessed 12 August 2012

Olsen S, 'Geographic tracking raises opportunities, fears' (*CNET News*, 8 November 2000) <<http://news.cnet.com/2100-1023-248274.html>> accessed 6 July 2012

Olsen S, 'Digital Envoy wins geotargeting patent' (*CNET News*, 29 June 2004) <http://www.news.cnet.com/Digital-Envoy-wins-geotargeting-patent/2110-1032_3-5251844> accessed 30 June 2010

OpenNet Initiative, 'Saudi Arabia' (2009) <<https://opennet.net/research/profiles/saudi-arabia>> accessed 14 May 2014

Patry W, 'Can a Minor be Sued for Infringement?' (*The Patry Copyright Blog*, 28 September 2006) <<http://williampatry.blogspot.co.uk/2006/09/can-minor-be-sued-for-infringement.html>> accessed 15 August 2012

Penn Computing, 'IPv6 (Internet Protocol version 6) at Penn' (*University of Pennsylvania*) <<http://www.upenn.edu/computing/ipv6/>> accessed 14 August 2012

Pinsent Mason LLP, 'Voluntary Copyright Alert Programme could be operational before end of 2014, says UK government' (*Out-Law*, 24 March 2014) <<http://www.out-law.com/en/articles/2014/march/voluntary-copyright-alert-programme-could-be-operational-before-end-of-2014-says-uk-government/>> accessed 21 May 2014

PT Shamrock, 'PT Freedom Phone™- Anonymous Mobile & (GSM) Sim Card – The hassle of anonymous call sending and receiving SOLVED' <<http://www.ptshamrock.com/auto/freedomphone.htm>> accessed 5 July 2012

Quova, 'Technical Overview of GeoPoint' <http://www.quova.com/technology/quova_tech_whitepaper.pdf> accessed 30 June 2010

RIPE, 'Welcome to the RIPE Network Coordination Centre' <www.ripe.net> accessed 14 August 2012

Schneier B, 'Anonymity and the Internet' (*Schneier on Security*, 3 February 2010) <http://www.schneier.com/blog/archives/2010/02/anonymity_and_t_3.html> accessed 3 July 2012

Schneier B, 'Schneier on Security' <<http://www.schneier.com/>> accessed 3 July 2012

Smith CS, 'Geolocation: Core to the Local Space and Key to Click-Fraud Detection' (*Search Engine Land*, 13 August 2007) <<http://searchengineland.com/geolocation-core-to-the-local-space-and-key-to-click-fraud-detection-11922>> accessed 6 July 2012

Stankey B, 'UK ISPs to begin storing Internet traffic data' (*ACC*, 19 February 2009) <<http://www.lexology.com/library/detail.aspx?g=0abfe79d-00a2-4532-8dea-5e6281efef64>> accessed 16 April 2014

Sterling JAL, 'Draft International Copyright Code' (May 2001) <http://www.qmipri.org/documents/icc_english.pdf> accessed 13th August 2012

Superb Internet, 'Study: Where the Web is located and Ghost Servers Haunting the Internet' (24 May 2013) <<http://www.superb.net/blog/2013/05/24/study-where-the-web-is-located-ghost-servers-haunting-the-internet/>> accessed 10 June 2014

'The Brussels I Regulation (No 44/2001)' (*Dutch Civil Law*)
<<http://dutchcivillaw.com/content/brusselone022.htm>> accessed 15 August 2012

The Parliament of the Commonwealth of Australia, 'Interactive Gambling Bill 2001 Revised Explanatory Memorandum' (1998-1999-2000-2001)
<http://www.archive.dcita.gov.au/__data/assets/pdf_file/0016/11536/Interactive_Gambling_Bill_2001_Revised_Explanatory_Memorandum.pdf> accessed 14 August 2012

Whittaker Z, "'Censorship creep": Pirate Bay block will affect one-third of U.K.' (*CNET*, 16 June 2012) <http://news.cnet.com/8301-1023_3-57454683-93/censorship-creep-pirate-bay-block-will-affect-one-third-of-u.k/> accessed 14 May 2014

WIPO, 'Contracting Parties Berne Convention'
<http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15> accessed 29 May 2014.

WIPO, 'Contracting Parties Paris Convention'
<http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=2> accessed 29 May 2014

WIPO, 'The Role of Private International Law and Alternative Dispute Resolution'
<http://www.wipo.int/copyright/en/ecommerce/ip_survey/chap4.html#_ftn432>
accessed 1 July 2012

Yinan Z 'Online IPR infringement cases on the rise' (*China Daily*, 20 December 2011)
<http://www.chinadaily.com.cn/china/2011-12/20/content_14294110.htm> accessed 24 June 2012

<<http://janus.fernuni-hagen.de>>

<<http://where-is.info/>>