

# Table of Contents

<i>Table of Cases</i>	xxi
<i>Table of Legislation</i>	xxxix
1. A Brief Introduction	1
2. “Head in the Clouds”: The Clash between Territorial Sovereignty, Jurisdiction, and the Territorial Detachment of the Internet	4
1. Different contexts of the term “jurisdiction”	4
2. State sovereignty	7
3. State sovereignty, national identity in the context of globalization	10
4. Global law?	15
5. Nexus to territory: territoriality, interests, and connecting factors; extraterritoriality	20
3. The Jurisdictional Challenge Answered—Enforcement through Gatekeepers on the Internet	33
1. The “out-of-reach” problem	33
2. Internet gatekeepers as facilitators of illegal activity?	35
3. Online service provider liability as gatekeepers?	36
4. The use of gatekeeper legislation for specific types of content	41
4.1 Hosting: from notice and take down to duty of care	41
4.1.1 CSEA materials	41
4.1.2 Terrorism-related materials	42
4.1.3 Online gambling and notice and take down	49
4.1.4 Wider range of contents	50
4.1.4.1 The German Netzwerkdurchsetzungsgesetz (NetzDG)	50
4.1.4.2 Audiovisual Media Services Directive (EU) 2018/1808	53
4.1.4.3 The UK White Paper “Online Harms” 2019	56
4.1.4.4 Australia	58
4.1.4.4.1 Schedules 5 and 7 Broadcasting Services Act 1992	58
4.1.4.4.2 Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019	58
4.1.5 Content regulation point two: hosting as gatekeeping	61
4.2 Internet access providers as local gatekeepers—blocking	65
4.2.1 Blocking of CSEA	67
4.2.2 Blocking of terrorist content	67
4.2.3 Pornography and the Digital Economy Act 2017	68
4.2.4 Website blocking and gambling	68
4.2.5 UK White Paper “Online Harms” and website blocking	69
4.2.6 Australia and internet access blocking	70

4.3 Payment services providers, advertisers, and search engines as gatekeepers	70
4.3.1 Digital Economy Act 2017 and the White Paper “Online Harms”	71
4.3.2 Payment blocking of illegal gambling payments	71
5. Conclusion	78
4. Criminal Jurisdiction—Concurrent Jurisdiction, Sovereignty, and the Urgent Requirement for Coordination	81
<i>Julia Hörnle and Elif Mendos Kuskonmaz</i>	
1. Introduction	81
2. Jurisdiction under (public) international law	82
2.1 The territoriality principle and effects doctrine	83
2.2 Principles of extraterritorial jurisdiction	87
2.2.1 Personality principle	87
2.2.2 Protective principle	89
2.2.3 Universality principle	89
3. Developing principles for cybercrime: territorial and extraterritorial laws	90
3.1 Territoriality principle in exercising jurisdiction over cybercrimes	91
3.2 Extraterritorial laws in prescribing cybercrimes	95
4. Resolving jurisdiction conflicts for cybercrimes: limiting the assertion of jurisdiction and coordinating criminal enforcement	96
4.1 International comity and the reasonableness principles	96
4.2 EU criminal law coordination	99
5. <i>Ne bis in idem</i> , the rule against double jeopardy	107
6. Conclusion	113
5. Jurisdiction of the Criminal Courts in Cybercrime Cases in Germany and England	115
1. Jurisdiction under German criminal law	116
1.1 Introduction	116
1.2 Territoriality principle as the main basis for jurisdiction	117
1.3 Protecting particular German interests, frequently combined with the active and passive personality principle for a limited number of specified offences (protective principle)	122
1.3.1 National state interests	123
1.3.2 German public interests	125
1.3.3 Protection of individual interests	126
1.4 Universality principle (Weltrechtsprinzip)	127
1.5 Passive personality principle	130
1.6 Active personality principle	131
1.7 Representation principle	132
2. Jurisdiction under English criminal law	132
2.1 Prevalence of territoriality principle	132
2.2 The terminatory approach or last act rule	136
2.3 Substantial measure test	137
2.4 Inchoate offences	140
2.5 Computer misuse offences and jurisdiction	141
3. Conclusion	143

6. Digital Investigations in the Cloud—Criminal Enforcement Cooperation	145
1. Introduction	145
2. International cooperation and digital investigations	151
2.1 Ad hoc cooperation and treaty-based international cooperation: MLA	151
2.2 The Cybercrime Convention: multilateral cooperation	159
3. Intra-EU cooperation in digital investigations	163
3.1 Mutual recognition and mutual trust in the EU: how does criminal enforcement jurisdiction in the EU legal order relate to fundamental rights?	163
3.2 Specific instruments for EU cooperation in the field of digital investigations	170
3.2.1 European Investigation Order	170
3.2.2 Joint investigation teams (JITs)	175
3.2.3 Intra-EU institutional cooperation	177
3.2.3.1 Europol and Europol's Cybercrime Centre	177
3.2.3.2 Eurojust	177
4. Export of data from the EU	179
4.1 The EU legal framework and its workarounds	179
4.1.1 Adequacy	180
4.1.2 Other safeguard mechanisms	182
4.1.3 Derogations	183
4.2 The different permutations of the dilemma	188
4.3 Safe Harbor, the Privacy shield and <i>Schrems I</i> and <i>II</i>	191
4.4 US–EU Umbrella Framework Agreement	195
5. Cross-border access to data for digital investigations—extending jurisdiction under international law?	197
5.1 Using coercive powers under domestic criminal procedures	197
5.1.1 Domestic criminal procedures achieving direct disclosure of foreign stored data by ISPs	197
5.1.1.1 Domestic ISP controls data, but not data in foreign locations, US <i>Microsoft case</i> and the Cloud Act	198
5.1.1.2 Foreign ISP controls data in foreign locations	201
5.1.1.3 Guidance Note interpretation of Article 18 Production Orders	203
5.1.2 Remote search and seizure and the use of OSINT authorized under domestic criminal procedures	206
5.1.2.1 Remote search and seizure—hacking by law enforcement	206
5.1.2.2 Access to open source materials: Article 32(a) of the Cybercrime Convention	209
5.2 Extending jurisdiction through international agreement for disclosure of data	211
5.2.1 The Cloud Act and executive agreements	211
5.2.2 The EU E-Evidence Regulation (Proposal)	215
5.3 Voluntary disclosure by ISPs	220
5.3.1 Direct, “voluntary” informal cooperation with foreign service providers	220



5.3.2 Access—voluntary and lawful: Article 32(b) Cybercrime Convention	222
6. Data sovereignty and data localization	223
7. Digital investigations, jurisdiction, and fundamental rights of citizens	226
8. Conclusion	230
7. Data Protection Regulation and Jurisdiction	233
1. Introduction	233
2. Applicable law versus jurisdiction	235
3. Specific rules on the competence of the supervisory authorities in EU data protection law	237
3.1 Data Protection Directive 1995/46/EC	237
3.2 GDPR EU/2016/679	240
3.2.1 One stop shop	240
3.2.2 Competence of data protection authorities—jurisdiction	241
3.2.3 Cooperation obligation of the Member States, the consistency mechanism and the EDPB	242
4. Rules on applicable law	243
4.1 Establishment link in the Directive and the Regulation	244
4.1.1 The concept of establishment in the jurisprudence of the CJEU	245
4.1.2 In the context of the activities of an establishment of the controller	246
4.2 Equipment as a territorial link	250
4.3 Domain names as a jurisdictional link and geo-blocking	251
4.4 Residency as a further requirement before EU data protection law applies	253
4.5 Targeting link in the Regulation	254
4.6 Application of EU law/Member States' law by virtue of public international law	255
5. General principles	255
5.1 The territoriality principle and the effects test	256
5.2 The protective principle under international law	258
5.3 The “country of origin” regulation principle	259
5.4 The “country of destination” regulation principle, consumer protection law, and the targeting principle	260
6. Conclusion	261
8. Civil and Commercial Cases in the EU: Jurisdiction, Recognition, and Enforcement, Applicable Law—Brussels Regulation, Rome I and II Regulations	264
<i>Julia Hörnle and Ioannis Revolidis</i>	
1. Introduction	264
1.1 The internet challenge and EU private international law	264
1.2 Some core principles of EU private international law	265
1.3 The UK's position after Brexit	268
2. Scope of application and general rules of jurisdiction and law applicable	269
2.1 Civil and commercial matters	269

2.2	The cross-border character of a case	269
2.3	Scope of application	270
2.4	The contractual or non-contractual character of a case	271
2.5	The relationship of EU private international law with the “principle of country of origin” established in Article 3 E-Commerce Directive	272
2.6	General rule of jurisdiction under the Brussels Ibis Regulation	272
2.7	Choice as a conflict of laws rule for contractual obligations under the Rome I Regulation	273
2.8	General conflict of laws rule for non-contractual obligations under the Rome II Regulation	275
3.	Special EU rules of jurisdiction and law applicable for contractual obligations	276
3.1	Overview	276
3.2	Prorogation under Article 25 Brussels Ibis	276
3.3	Jurisdiction—special rule of Article 7(1) Brussels Ibis	278
3.4	Choice of law—Article 4 Rome I	284
4.	Special EU rules for jurisdiction and law Applicable for non-contractual obligations	284
5.	<i>Lis pendens</i> and related actions	286
6.	Recognition and enforcement	287
9.	Conflicts of Law and Internet Jurisdiction in the US	289
1.	Introduction	289
2.	Adjudicative jurisdiction and US principles	290
2.1	The Constitutional due process clauses and long-arm statutes	290
2.2	“Minimum contacts” and notions of fair play and substantial justice	293
2.3	Personal jurisdiction: general and specific	296
3.	<i>In rem</i> and <i>quasi in rem</i> jurisdiction	299
4.	Internet cases: jurisprudence	300
4.1	Specific personal jurisdiction	300
4.2	<i>Calder v Jones</i> and “effects doctrine”	305
4.3	Stream of commerce cases	309
4.4	Jurisdiction clauses in contracts	311
5.	Additional principles: forum non-convenience, comity, and reasonableness	313
6.	Procedural jurisdiction from a US perspective	322
7.	Conclusion	328
10.	Consumer Protection and Jurisdiction	331
1.	Introduction	331
2.	The approach to forum selection and consumer protection in the US	333
2.1	The contractual analysis: party autonomy and mutuality in the US	333
2.2	Unconscionable clauses in adhesion contracts: procedural and substantive unconscionability (incorporation and fairness)	336
2.2.1	Procedural unconscionability	337
2.2.2	Substantive unconscionability	340

2.3	Contravening strong public policy in the forum	341
2.4	Conclusion: US law	344
3.	EU consumer jurisdiction	345
3.1	A brief history of the harmonization of the rules on private international law and special consumer protection in the EU	345
3.2	Consumer protection rules in private international law in the EU	347
3.3	Interpretation by the CJEU	352
3.3.1	Who is a consumer and when is a contract concluded?	353
3.3.2	Closely linked contracts	357
3.3.3	Interaction of the consumer jurisdiction rules and the national civil procedure rules in determining the venue	359
3.3.4	The directing/targeting rule and e-commerce	361
4.	Conclusion	367
11.	Conflicts of Law in Privacy, Data Protection, and Defamation Disputes: German and English Law	369
1.	Introduction	369
2.	Jurisdiction	370
2.1	Harmonized rules on jurisdiction in the Brussels (Recast) Regulation	370
2.2	Jurisdictional rules in the General Data Protection Regulation	378
2.3	Jurisdiction under German law	380
2.4	Rules of jurisdiction under English common law	386
2.5	Conclusion: jurisdiction	392
3.	Applicable law	393
3.1	Applicable law under the Rome II Regulation on the Law Applicable to Non-Contractual Obligations	393
3.2	Applicable law under German law	394
3.3	Applicable law under English law	396
3.3.1	Applicable law to personality rights infringements other than defamation	397
3.3.2	Applicable law to defamation	399
3.3.3	Conclusion: applicable law	402
4.	Conclusion	403
12.	Intellectual Property—Internet Jurisdiction and Applicable Law	406
1.	Intellectual property and territoriality	406
2.	Domain names and <i>in rem</i> jurisdiction	408
3.	Jurisdiction in the EU and UK	411
3.1	Harmonized EU jurisdiction rules and IP	412
3.1.1	Personal jurisdiction—special tort rule in IP infringement cases	413
3.1.2	<i>In rem</i> , subject-matter jurisdiction and its interplay with personal jurisdiction	418
3.2	English jurisdiction rules	420
3.3	Recent developments, unregistered rights, and subject-matter jurisdiction	420



3.4 The EU Trademark Regulation, Community Design Regulation and European patent	423
3.4.1 The EU Trademark Regulation and Community Design Regulation	423
3.4.2 European patents	428
4. Applicable law in the EU and UK	429
4.1 Rome Regulation	429
4.2 Copyright: Berne Convention	431
4.3 Caselaw of the English courts	433
5. Conclusion	434
13. Conclusion	436
1. Jurisdiction and disruptive technologies—the jurisdictional challenge	436
2. Globalization and identity	437
3. Connecting factors and territoriality	437
4. Worldwide remedies or localized remedies?	440
5. Enforcement: the role of private gatekeepers	441
6. Changing the territoriality principle: closed systems and their interfaces	442
7. Rule-level changes	443
7.1 Targeting and directing	443
7.2 Jurisdictional restraint: comity, extraterritoriality, and reasonableness	446
8. Systemic changes	446
8.1 Coordination, coordination, coordination	447
8.2 Geo-location and geo-blocking	448
8.3 Private law systems: depleting sovereignty and states within states	450
9. The relationship between jurisdiction, the rule of law, and fundamental rights	451
<i>Index</i>	453