
Contents

1	Legal Foundations	1
1.1	Purpose and Principles of Law	1
1.1.1	Salmond on the Classifications of Law	2
1.1.2	The Rule of Law	2
1.2	Jurisprudence	4
1.2.1	Natural Law Jurisprudence: Observation and Realization	5
1.2.2	Analytical Jurisprudence: Definition and Clarification	6
1.2.3	Normative Jurisprudence: Evaluation and Reformation	9
1.3	Sources of Law	10
1.3.1	Legislation/Statutory Law	10
1.3.2	Legal Precedent/ Case Law/Common Law	11
1.3.3	Sources of Legal Influence	12
1.4	Systems of Law	13
1.4.1	Common Law	14
1.4.2	Civil Law	14
1.4.3	Religious Law	15
1.4.4	Customary Law	16
1.4.5	Legal Pluralism	16
1.4.6	Case Hypothetical: Systems of Law	16
1.5	Categories of Law	17
1.5.1	International Law vs Domestic Law	17
1.5.2	Recognition of Sovereignty	18
1.5.3	Public Law versus Private Law	19
1.5.4	Case Hypothetical: Categories of Law	19
1.6	Legal Governance	20
1.6.1	Authoritarianism	21
1.6.2	Monarchism	24
1.6.3	Elitism	24
1.6.4	Socialism	25
1.6.5	Democracy	26
1.6.6	Case Hypothetical: Legal Governance	27

1.7	Constitutionalism	27
1.7.1	Division of Jurisdictional Powers	29
1.7.2	Branches of Legal Governance	30
1.8	Summary	31
	References	32
2	Property and Privacy in Context	37
2.1	Perceptions of Property	37
2.2	Ownership, Possession, and Interest	38
2.2.1	Distinguishing Ownership from Possession	38
2.2.2	Ownership	39
2.2.3	Possession	39
2.2.4	Interest	41
2.2.5	Case Hypothetical: Ownership, Possession, and Interest	43
2.3	Property and Privacy	44
2.3.1	Classifications of Property	45
2.3.2	Private Property Versus Public Property	47
2.3.3	Privacy	47
2.3.4	Differentiating Personal from Private	47
2.3.5	Legislative Example: Canadian Consumer Privacy Protection	49
2.3.6	Case Hypothetical: Consumer Privacy Protection	50
2.4	The Intersection of Property, Privacy, and Cybersecurity Law	51
2.4.1	Criminal Law/Statutory Law	52
2.4.2	Tort Law/Common Law	53
2.4.3	Case Hypothetical: Intersection of Criminal and Tort Law	53
2.5	Summary	55
	References	56
3	Cybersecurity and Cybercrimes	59
3.1	Categorizing Cybercrimes	59
3.1.1	Cyber-Enabled Offences (On/Offline)	60
3.1.2	Cyber-Dependent Offences (Online)	65
3.1.3	Computer/Cyber-Supported Offences	80
3.1.4	National (Cyber)Security Offences	85
3.2	Growing Prevalence of Cybercrime	91
3.3	Categorizing Cybercrimes in the Law	91
3.4	Summary	93
	References	95
4	Global Relevance	97
4.1	Review of Canadian Cybersecurity Laws	98
4.1.1	Regulating Governmental Relationships	98

4.1.2	Regulating Businesses, Organizations, and Commercial Enterprises	99
4.1.3	Regulating Interpersonal Relationships and Criminal Activities	100
4.2	Review of Australian Cybersecurity Laws	102
4.2.1	Regulating Governmental, Business, and Organizational Relationships	102
4.2.2	Regulating Interpersonal Relationships and Criminal Activities	105
4.3	Review of United Kingdom Cybersecurity Laws	108
4.3.1	Regulating Government, Businesses, and Organizations	108
4.3.2	Regulating Interpersonal Relationships and Criminal Activities	109
4.4	Review of United States Cybersecurity Laws	110
4.4.1	Regulating the Federal Government and Governmental Agencies	111
4.4.2	Regulating Sector-Specific Industries: Healthcare	111
4.4.3	Regulating Sector-Specific Industries: Banks/Financial Institutions	112
4.4.4	Regulating Interpersonal Relationships and Criminal Activities	113
4.5	Common Law Countries, in Brief	114
4.6	National Considerations	115
4.6.1	Identity and Diversity	115
4.6.2	Identity in Politics	118
4.6.3	Constitutional Values	121
4.7	International Considerations	121
4.7.1	Treaties and International Agreements	123
4.7.2	The <i>Tallinn Manual</i> and Cyber Warfare	125
4.7.3	International Legal Principles in Cyberspace	133
4.7.4	International Dispute Resolution	133
4.8	Summary	135
	References	135
5	Emerging Issues	137
5.1	Globalization and Jurisdictionally	137
5.1.1	Determining Jurisdiction	138
5.1.2	Online Jurisdiction	139
5.1.3	Case Hypothetical: Jurisdiction	139
5.2	Digital Marketplaces and the Consumer	142
5.2.1	Rights of the Consumer in the Global Marketplace	142
5.2.2	Commercial Electronic Messages	144
5.2.3	International Commercial Application	146
5.3	Anonymized DarkNet Markets and Cryptocurrencies	148
5.3.1	Illegal Content and Dark Web Marketplaces	150

5.3.2	Differentiating the Dark from the Deep	153
5.3.3	Cryptocurrencies	159
5.3.4	Corporate Considerations	160
5.4	Challenges to Law Enforcement	165
5.4.1	Decentralization	166
5.4.2	Detection, Tracing and Localization	166
5.4.3	Jurisdiction and Enforcement	168
5.4.4	Digital Evidence Collection	168
5.4.5	Example in Law: Canada’s Evidence Act	169
5.4.6	Case Hypothetical: Challenges to Law Enforcement	170
5.5	Digital Sovereignty and Data Governance	171
5.5.1	Challenges to Digital Sovereignty in International Cyber Law	171
5.5.2	Online Content Regulation	172
5.5.3	Digital Content Creation and the Gig Economy	172
5.6	Future Directions	175
5.7	Summary	175
	References	176
	Conclusion	179