

Table of Contents

<i>Preface</i>	v
<i>Table of Cases</i>	xix

PART ONE

Introduction to Cybercrime and the Regulation of Cyberspace

<i>Chapter 1: Introduction to Cyberspace and Cybercrime</i>	3
Introduction.....	3
The Internet’s Unique Layered Architecture.....	9
The Anatomy of a Computer.....	11
Macs vs. PCs.....	11
Cyberspace and Criminal Activity	14
Facts & Figures: How Prevalent is Cybercrime and What Challenges Does It Pose?	16
Cybercrime in Numbers.....	16
The Complex Nature of Today’s Cyber-Threats.....	19
Conclusion	25
Questions for Further Thinking and Discussion	26
 <i>Chapter 2: Introduction to the Regulation of Cyberspace</i>	27
Introduction.....	27
Cyberspace as a Unique Place	28
Regulation in Cyberspace	35
Conclusion	40
Questions for Further Thinking and Discussion	40

PART TWO

Traditional Crime in Cyberspace

<i>Chapter 3: Identity Theft and Cyber Fraud</i>	45
Introduction.....	45
What is Fraud?	47
Common Cyber Methods Of Perpetrating Fraud.....	48
What is Identity Theft?	52
Common Cyber Methods of Perpetrating Identity Theft.....	53
Costs of Identity Theft and Fraud	65
The Underground Economy and Organized Crime	68
Credit Card Information and the Underground Economy	72

Policy Approaches to Identity Theft	73
Legislation to Combat Identity Theft.....	74
Privacy Legislation	81
Data Breach Notification Legislation	82
Conclusion	85
Questions for Further Thinking and Discussion	85
Chapter 4: Child Sexual Abuse and the Internet	87
Introduction.....	88
The History of Online Child Pornography	89
What is the Content of Child Pornography?	91
How Much Child Pornography is There?	94
How Do Child Pornography Offenders Use the Internet?	96
Web-Based Materials	99
Peer-to-Peer (P2P) Networks.....	100
TOR and The Dark Web	102
Online Support Networks	104
The Legal Definition of Child Pornography	106
Child Pornography and Freedom of Expression.....	107
<i>R. v. Sharpe</i> and Subsequent Legislative Initiatives	110
The Detection and Apprehension of Offenders.....	119
Canada’s National Strategy Against Internet Child Sexual Exploitation	119
Individuals and Mandatory Child Pornography Reporting Laws in Canada	120
ISPs and Filtering and Blocking.....	122
The Need for International Cooperation	123
The Importance of International Conventions	123
An International Law Enforcement Network	125
Child Luring.....	128
The Nature of Child Luring Incidents.....	129
Child Luring and the Law in Canada.....	133
Online Sting Operations and Child Luring Cases.....	136
Conclusion	137
Questions for Further Thinking and Discussion	137
Chapter 5: Bullying, Stalking and Harassment on the Internet	139
Introduction.....	139
An Overview Of Cyber-Bullying.....	140
Cyber-Bullying and the Law in Canada.....	144
Provincial Policy Initiatives and Legislation	144
Federal Policy Initiatives and Legislation	146

Bullying and the <i>Criminal Code</i>	147
Criminal Harassment – Sections 264 and 264.1 of the <i>Criminal Code</i>	148
Harassing Communications – Subsection 372(3) of the <i>Criminal Code</i>	150
Canadian Human Rights Law	151
A Note on Canadian Law and Hate Speech on the Internet.....	151
Cyber-Harassment And Cyber-Stalking.....	153
Conclusion	158
Questions for Further Thinking and Discussion	158

PART THREE
Computer Misuse Crimes

Chapter 6: Viruses and Other Malicious Programs	163
Introduction.....	163
Malware Terms	164
Malware Threats Today: PC vs. MAC.....	169
How is Malware Distributed?	170
Web-Based Attacks	170
Email-Borne Malware.....	172
Social Networking Malware	173
Mobile Code and Mobile Malware.....	173
The Android Platform	174
The iOS Platform	175
Virtual Environments/Cloud Computing.....	175
Cyber-Espionage and Advanced Persistent Threats	176
The Online Underground Economy.....	179
Policy Responses to Malware	179
Conclusion	181
Questions for Further Thinking and Discussion	181
 Chapter 7: Hacking and Denial of Service Attacks	183
Introduction.....	183
Phone Phreaking: The Precursor to Hacking	184
The Definition of Hacking – A Form of Spying and Intrusion	185
Methods of Hacking – Digital Spying and Intrusions Explained	186
Password Cracking	186
Packet Sniffing and War Driving.....	187
Port Scanning.....	187
Scareware.....	188
Spyware and Keystroke Loggers.....	188
Hacking Android and iOS Devices.....	189

Social Engineering – The Art of the Con	189
Hacker Subculture and Hacker Ethics	191
Hacker Typologies and Hacker Motivations.....	191
The Culture of Hacking	193
Preventing and Managing Hacking – Regulatory and Non-Regulatory Measures	196
Denial of Service and Distributed Denial of Service Attacks.....	199
Denial of Service (DoS) Attacks.....	199
Distributed Denial of Service (DDoS) Attacks.....	200
Conclusion	201
Questions for Further Thinking and Discussion	201
 <i>Chapter 8: Spam in Cyberspace</i>	203
INTRODUCTION	203
How Significant is the Spam Problem?	205
How Is Spam Distributed?	206
Bot Networks	206
URL Shortening	207
Social Media	207
Spear-Phishing	208
Malicious Software	209
Social Engineering/Phishing Scams	209
What’s Wrong with Spam?	210
Spam Laws In Canada	211
Canadian Legislation Dealing With Spam.....	211
Canadian Jurisprudence Dealing With Spam.....	217
Non-Legal Measures to Combat Spam	218
Conclusion	219
Questions for Further Thinking and Discussion	220

PART 4

Specific Problems with the Regulation and Prosecution of Cybercriminals

<i>Chapter 9: International Jurisdiction and the Regulation of Cyberspace</i> ...	223
Introduction.....	223
Specific Measures for Effective Inter-Jurisdictional Cooperation.....	224
The Importance of International Conventions	224
The Importance of Capacity Building and International Cooperation	230
Conclusion	234
Questions for Further Thinking and Discussion	235

<i>Chapter 10: Searching and Seizing Evidence in Cyberspace</i>	237
Introduction.....	237
The Privacy And <i>Charter</i> Implications Of Electronic Surveillance.....	238
<i>The Canadian Charter of Rights and Freedoms</i>	238
Introduction to Electronic Evidence	246
Introduction to Computer Forensic Investigations	247
ISPs and Lawful Access to Information In Canada	249
Access to Subscriber Information.....	249
Intercept Capability.....	250
Orders for the Preservation of Data	252
Orders for the Production of Data.....	253
The <i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i>	254
Conclusion	254
Questions for Further Thinking and Discussion	255
 <i>Chapter 11: Emerging Trends and Future Concerns</i>	 257
Introduction.....	257
Emerging Trends and Future Concerns	258
Conclusion	259
Questions for Further Thinking and Discussion	260
 <i>Glossary</i>	 261
<i>Index</i>	277