Cybercrime In Canadian Criminal Law

RILEY SARIAH

Cybercrime American Bar Association
Police services around the world are embarking on a major period of change that has seen few parallels since the founding of modern policing in the 19th century. A conflation of factors some long-standing, others of more recent origin, but all significant – are now coalescing, with implications for the traditional ways in which police services have been providing safety and security for the public. Today, there are many actors who help ensure a safe and secure environment, including technical specialists, public and private security providers, and first responders. As such, police have begun to work within a safety and security web that requires new and dynamic partnerships, flexibility, and adaptability. In addition, police are addressing increasingly complex and global crimes such as terrorism, identity theft, and cybercrime. These challenges, along with increasing costs, have led many around the world and in Canada to re-examine the traditional policing model and consider what modern approaches are required to ensure effective and efficient policing for the future.
Canadian Communication Policy and Law Routledge
Cybersecurity, data privacy law, and the related legal implications overlap into a relevant and developing area in the legal field. However, many legal practitioners lack the foundational understanding of computer processes which are fundamental for applying existing and developing legal structures to the issue of cybersecurity and data privacy. At the same time, those who work and research in cybersecurity are often unprepared and unaware of the nuances of legal application. This book translates the fundamental building blocks of data privacy and (cyber)security law into basic knowledge that is equally accessible and educational for those working and researching in either field, those who are involved with businesses and organizations, and the general public.
Computer-related Crime Routledge
The SARS-CoV-2 pandemic has had an undeniable impact on cybercrime. The initial crisis quickly became a global catastrophe with multiple consequences in economics, health, and political and social fields. This book explores how this global emergency has influenced cybercrime. Indeed, since feeding off new vulnerabilities, thanks to the effects of the pandemic crisis in various states around the world, cybercrime has increased and evolved. In 2020, the world was already dealing with numerous tensions and the effects of the global crisis have therefore only tended to exacerbate the issues that relate to cybercrime. For example, radicalization and identity theft has found an environment in which they thrive: the Internet. Criminals have been able to adapt their modus operandi, their targets and their attack vectors. However, on the plus side, the response of law enforcement and public authorities, in terms of the legal, policing and policy side of cybercrime, has also been adapted in order to better combat the increase in this phenomenon.
Wayward Dragon Springer Nature
Digital technology has transformed the way in which we socialise and do business. Proving the maxim that crime follows opportunity, virtually every advance has been accompanied by a corresponding niche to be exploited for criminal purposes; so-called 'cybercrimes'. Whether it be fraud, child pornography, stalking, criminal copyright infringement or attacks on computers themselves, criminals will find ways to exploit new technology. The challenge for all countries is to ensure their criminal laws keep pace. The challenge is a global one, and much can be learned from the experience of other jurisdictions. Focusing on Australia, Canada, the UK and the USA, this book provides a comprehensive analysis of the legal principles that apply to the prosecution of cybercrimes. This new edition has been fully revised to take into account changes in online offending, as well as new case law and legislation in this rapidly developing area of the law.
Computer Forensics and Cyber Crime Cambridge University Press
This is the first book to present a multidisciplinary approach to cyberterrorism. It traces the threat posed by cyberterrorism today, with chapters discussing possible technological vulnerabilities, potential motivations to engage in cyberterrorism, and the challenges of distinguishing this from other cyber threats. The book also addresses the range of potential responses to this threat by exploring policy and legislative frameworks as well as a diversity of techniques for deterring or countering terrorism in cyber environments. The case studies throughout the book are global in scope and include the United States, United Kingdom, Australia, New Zealand and Canada. With contributions from distinguished experts with backgrounds including international relations, law, engineering, computer science, public policy and politics, Cyberterrorism: Understanding, Assessment and Response offers a cutting edge analysis of contemporary debate on, and issues surrounding, cyberterrorism. This global scope and diversity of perspectives ensure it is of great interest to academics, students, practitioners, policymakers and other stakeholders with an interest in cyber security.
Cybercrime During the SARS-CoV-2 Pandemic John Wiley & Sons
This concise volume takes care of two major issues at once; providing readers with a more worldwide view than American-centric information, and educating readers about cybercrime. This volume of essays from international sources explores the vulnerability of countries and people to cybercrime. Readers will explore cybercrime law worldwide, and take a look at the role of organized crime in cybercrime. They will also take a deep dive into cyber espionage and cyber terrorism. Countries and cultures that readers will learn about include South Africa, Singapore, Pakistan, China, Canada, Thailand, Australia, Russia, and the United Kingdom.
Cyberterrorism Greenhaven Publishing LLC
A comprehensive doctrinal analysis of cybercrime laws in four major common law jurisdictions: Australia, Canada, the UK and the US.
Cybercrime in Context Routledge
Online Version - Discusses current cybercrime laws and practices. Available online for downloading.
International & Transnational Criminal Law Scarborough, Ont. : Carswell
Cybercrime, also called computer crime, the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially through the Internet, has grown in importance as the computer has become central to commerce, entertainment, and government.Because of the early and widespread adoption of computers and the Internet in the United States, most of the earliest victims and villains of cybercrime were Americans. By the 21st century, though, hardly a hamlet remained anywhere in the world that had not been touched by cybercrime of one sort or another.New technologies create new criminal opportunities but few new types of crime. What distinguishes cybercrime from traditional criminal activity? Obviously, one difference is the use of the digital computer, but technology alone is insufficient for any distinction that might exist between different realms of criminal activity. Criminals do not need a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate someone's privacy. All those activities existed before the "cyber" prefix became ubiquitous. Cybercrime, especially involving the Internet, represents an extension of existing criminal behaviour alongside some novel illegal activities.Most cybercrime is an attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. In other words, in the digital age our virtual identities are essential elements of everyday life: we are a bundle of numbers and identifiers in multiple computer databasesowned by governments and corporations. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity.An important aspect of cybercrime is its nonlocal

character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. For example, if a person accesses child pornography located on a computer in a country that does not ban child pornography, is that individual committing a crime in a nation where such materials are illegal? Where exactly does cybercrime take place? Cyberspace is simply a richer version of the space where a telephone conversation takes place, somewhere between the two people having the conversation. As a planet-spanning network, the Internet offers criminals multiple hiding places in the real world as well as in the network itself. However, just as individuals walking on the ground leave marks that a skilled tracker can follow, cybercriminals leave clues as to their identity and location, despite their best efforts to cover their tracks. In order to follow such clues across national boundaries, though, international cybercrime treaties must be ratified.In 1996 the Council of Europe, together with government representatives from the United States, Canada, and Japan, drafted a preliminary international treaty covering computer crime. Around the world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information on their customers' transactions and to turn this information over on demand. Work on the treaty proceeded nevertheless, and on November 23, 2001, the Council of Europe Convention on Cybercrime was signed by 30 states.

Cambridge University Press

The infusion of digital technology into contemporary society has had significant effects for everyday life and for everyday crimes. Digital Criminology: Crime and Justice in Digital Society is the first interdisciplinary scholarly investigation extending beyond traditional topics of cybercrime, policing and the law to consider the implications of digital society for public engagement with crime and justice movements. This book seeks to connect the disparate fields of criminology, sociology, legal studies, politics, media and cultural studies in the study of crime and justice. Drawing together intersecting conceptual frameworks, Digital Criminology examines conceptual, legal, political and cultural framings of crime, formal justice responses and informal citizen-led justice movements in our increasingly connected global and digital society. Building on case study examples from across Australia, Canada, Europe, China, the UK and the United States, Digital Criminology explores key questions including: What are the implications of an increasingly digital society for crime and justice? What effects will emergent technologies have for how we respond to crime and participate in crime debates? What will be the foundational shifts in criminological research and frameworks for understanding crime and justice in this technologically mediated context? What does it mean to be a ‘just’ digital citizen? How will digital communications and social networks enable new forms of justice and justice movements? Ultimately, the book advances the case for an emerging digital criminology: extending the practical and conceptual analyses of ‘cyber’ or ‘e’ crime beyond a focus foremost on the novelty, pathology and illegality of technology-enabled crimes, to understandings of online crime as inherently social.

Computer Crime Springer

The growth of technology allows us to imagine entirely new ways of committing, combating and thinking about criminality, criminals, police, courts, victims and citizens. Technology offers not only new tools for committing and fighting crime, but new ways to look for, unveil, label crimes and new ways to know, watch, prosecute and punish criminals. This book builds on the work of Leman-Langlois' last book Technocrime, and brings together fresh perspectives from eminent scholars to consider how our relationship with technology and

Public Policing in the 21st Century Rothstein Publishing

Based on peer-reviewed articles from the Second International Conference of the South Asian Society of Criminology and Victimology, Interpersonal Criminology investigates the roots of crime and victimization, rather than dissecting criminal behavior after the fact. The book divides crime by type, covering crimes against women, crimes against children and youths, culture conflict and victimization of groups, and interpersonal cybercrimes. Perfect for criminal justice practitioners and advanced human rights, criminology, and victimology students, Interpersonal Criminology explores the complexities of crime and interpersonal events in both established and emerging fields of criminology, including those concerning women and minorities.

Guide to Cybersecurity Pearson Learning Solutions

This book brings together an international group of experts to present the latest psychosocial and developmental criminological research on cyberbullying, cybervictimization and intervention. With contributions from a wide range of European countries, including Cyprus, Greece, Ireland, Italy, France, Hungary, Spain, and the United Kingdom, as well as from Canada and the USA, this authoritative volume explores the nature, risk factors, and prevalence of cyberbullying among children and adolescents. A particularly original focus is directed towards the Tabby project (Threat Assessment of online Bullying Behaviour among Youngsters), an intervention programme based on the threat and risk assessment approach which seeks to prevent the occurrence of violence and its recidivism. Presenting cutting-edge research on developmental criminology and legal psychology, International Perspectives on Cyberbullying is a comprehensive resource for practitioners, teachers, parents, and researchers, as well as scholars of criminology, psychology, and education.

Technocrime, Policing, and Surveillance IGI Global

Cybercrime in Canadian Criminal Law

Right-Wing Extremism in Canada and the United States Council of Canadian Academies

Cybercrime: A Reference Handbook documents the history of computer hacking from free long distance phone calls to virtual espionage to worries of a supposed "cyber apocalypse," and provides accessible information everyone should know. An issue so new and evolving so quickly, there are few sources from which readers can get the information they need to inform themselves about and protect themselves from cybercrime. Written by experts in the field, this reference work contains original essays, descriptions of technical aspects, and numerous contributions from over 100 sources. Cybercrime uses fascinating case studies to analyze the beginning of cybercrime and the path it has followed to the present day. With biographical sketches of many influential hackers, the reader will better understand the development of the cybercriminal, and how many of these individuals went on to create some of the computer industry's most useful software. From cyberstalking to viruses, scholars and students alike will find the answers they need to understand these issues.

Policing Canada in the 21st Century: New Policing for New Challenges Routledge

However, as it is part of the "Essentials of Canadian Law" series, a major goal of the book is to explore fully the nexus between these bodies of international law and Canadian domestic law--and help Canadian courts and lawyers engage successfully with the international aspects of the cases they work on. Accordingly, the book contains: a stand-alone chapter on the prosecution of international crimes before Canadian courts; a detailed examination of how the various transnational crime treaties are implemented in Canadian law; and a full chapter on Canadian extradition and mutual legal assistance law and practice.

Criminal Int. Law - Convention on Cybercrime Pearson

"This book addresses various aspects of hacking and technology-driven crime, including the ability to understand computer-based threats, identify and examine attack dynamics, and find solutions"--Provided by publisher.

Digital Criminology Springer Nature

ASIS Book of The Year Runner Up. Selected by ASIS International, the world's largest community of security practitioners. In today’s litigious business world, cyber-related matters could land you in court. As a computer security professional, you are protecting your data, but are you protecting your company? While you know industry standards and regulations, you may not be a legal expert. Fortunately, in a few hours of reading, rather than months of classroom study, Tari Schreider’s Cybersecurity Law, Standards and Regulations (2nd Edition), lets you integrate legal issues into your security program. Tari Schreider, a board-certified information security practitioner with a criminal justice administration background, has written a much-needed book that bridges the gap between cybersecurity programs and cybersecurity law. He says, “My nearly 40 years in the fields of cybersecurity, risk management, and disaster recovery have taught me some immutable truths. One of these truths is that failure to consider the law when developing a cybersecurity program results in a protective façade or false sense of security.” In a friendly style, offering real-world business examples from his own experience supported by a wealth of court cases, Schreider covers the range of practical information you will need as you explore – and prepare to apply – cybersecurity law. His practical, easy-to-understand explanations help you to: Understand your legal duty to act reasonably and responsibly to protect assets and information. Identify which cybersecurity laws have the potential to impact your cybersecurity program. Upgrade cybersecurity policies to comply with state, federal, and regulatory statutes. Communicate effectively about cybersecurity law with corporate legal department and counsel. Understand the implications of emerging legislation for your cybersecurity program. Know how to avoid losing a cybersecurity court case on procedure – and develop strategies to handle a dispute out of court. Develop an international view of cybersecurity and data privacy – and international legal frameworks. Schreider takes you beyond security standards and regulatory controls to ensure that your current or future cybersecurity program complies with all laws and legal jurisdictions. Hundreds of citations and references allow you to dig deeper as you explore specific topics relevant to your organization or your studies. This book needs to be required reading before your next discussion with your corporate legal department. This new edition responds to the rapid changes in the cybersecurity industry, threat landscape and providers. It addresses the increasing risk of zero-day attacks, growth of state-sponsored adversaries and consolidation of cybersecurity products and services in addition to the substantial updates of standards, source links and cybersecurity products.

Cyber Security, Artificial Intelligence, Data Protection & the Law IGI Global

Certain types of crime are increasingly being perpetrated across national borders and require a unified regional or global response to combat them. Transnational criminal law covers both the international treaty obligations which require States to introduce specific substantive measures into their domestic criminal law schemes, and an allied procedural dimension concerned with the articulation of inter-state cooperation in pursuit of the alleged transnational criminal. The Routledge Handbook of Transnational Criminal Law provides a comprehensive overview of the system which is designed to regulate cross border crime. The book looks at the history and development of the system, asking questions as to the principal purpose and effectiveness of transnational criminal law as it currently stands. The book brings together experts in the field, both scholars and practitioners, in order to offer original and forward-looking analyses of the key elements of the transnational criminal law. The book is split into several parts for ease of reference: Fundamental concepts surrounding the international regulation of transnational crime. Procedures for international cooperation against alleged transnational criminals including jurisdiction, police cooperation, asset recovery and extradition. Substantive crimes covered by transnational criminal law analysing the current legal provisions for each crime. The implementation of transnational criminal law and the effectiveness of the system of transnational criminal law. With chapters from over 25 authorities in the field, this handbook will be an invaluable reference work for student and academics and for policy makers with an interest in transnational criminal law.

Research Paper on Computer Misuse Springer Nature

Losses attributed to criminal activities involving the use of computer systems are a subject of some controversy. No detailed study has ever been undertaken in Canada, in part because there is no consensus as to what exactly is a ċriminal activity involving the use of computer systems.' It is difficult to establish with any confidence the losses from computer crime without some clear conception of what such crime entails, and an accurate record of its frequency. This document presents a definition of computer crime. It looks at the significance of computer crime and Canadian criminal law respecting computers.