Cybercrime In Canadian Criminal Law

This edited book promotes and facilitates cybercrime research by providing a cutting-edge collection of perspectives on the critical usage of online data across platforms, as well as the implementation of both traditional and innovative analysis methods. The accessibility, variety and wealth of data available online presents substantial opportunities for researchers from different disciplines to study cybercrimes and, more generally, human behavior in cyberspace. The unique and dynamic characteristics of cyberspace often demand cross-disciplinary and cross-national research endeavors, but disciplinary, cultural and legal differences can hinder the ability of researchers to collaborate. This work also provides a review of the ethics associated with the use of online data sources across the globe. The authors are drawn from multiple disciplines and nations, providing unique insights into the value and challenges evident in online data use for cybercrime scholarship. It is a key text for researchers at the upper undergraduate level and above.

"This book is a vital compendium of chapters on the latest research within the field of distributed computing, capturing trends in the design and development of Internet and distributed computing systems that leverage autonomic principles and techniques"--Provided by publisher.

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.

Explaining cybercrime in a highly networked world, this book provides a comprehensive yet accessible summary of the history, modern developments, and efforts to combat cybercrime in various forms at all levels of government—international, national, state, and local. • Provides accessible, comprehensive coverage of a complex topic that encompasses identity theft to copyright infringement written for non-technical readers • Pays due attention to important elements of cybercrime that have been largely ignored in the field, especially politics • Supplies examinations of both the domestic and international efforts to combat cybercrime • Serves an ideal text for first-year undergraduate students in criminal justice programs

Crime and Justice in Digital Society

Researching Cybercrimes

Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century

The Strategies of Informing Technology in the 21st Century

Laws, Rights and Regulations

Cybercrime in Progress

"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.

"This book investigates cyber crime, exploring gendered dimensions of cyber crimes like adult bullying, cyber stalking, hacking, defamation, morphed pornographic images, and electronic blackmailing"--Provided by publisher.

Looking at the full range of cybercrime,and computer security he shows how the increase in personal computing power available within a globalized communications network has affected the nature of and response to criminal activities. We have now entered the world of low impact, multiple victim crimes in which bank robbers, for example, no longer have to meticulously plan the theft of millions of dollars. New technological capabilities at their disposal now mean that one person can effectively commit millions of robberies of one dollar each. Against this background, David Wall scrutinizes the regulatory challenges that cybercrime poses for the criminal (and civil) justice processes, at both the national and the international levels. Book jacket.

Online Version - Discusses current cybercrime laws and practices. Available online for downloading.

International Criminal Law

Routledge Handbook of Transnational Criminal Law

Theoretical Frameworks and Practical Applications

Cyber Crimes against Women in India

Criminal Int. Law - Convention on Cybercrime

The Oxford Handbook of Organized Crime

This timely book provides contributions on international, comparative crime phenomena: gangs, trafficking, fear of crime, and crime prevention. It highlights contributions originally prepared for the XVII World Congress of Criminology and for the 2015 Cybercrime Conference in Oñati, Spain which have been selected, reviewed, and adapted for inclusion in this volume. The work features international contributors sharing the latest research and approaches from a variety of global regions. The first part examines the impact of gangs on criminal activities and violence. The second part explores illegal trafficking of people, drugs, and other illicit goods as a global phenomenon, aided by the ease of international travel, funds transfer, and communication. Finally, international approaches to crime detection prevention are presented. The work provides case studies and fieldwork that will be relevant across a variety of disciplines and a rich resource for future research. This work is relevant for researchers in criminology and criminal justice, as well as related fields such as international and comparative law, public policy, and public health.

The emergence of the World Wide Web, smartphones, and Computer-Mediated Communications (CMCs) profoundly affect the way in which people interact online and offline. Individuals who engage in socially unacceptable or outright criminal acts increasingly utilize technology to connect with one another in ways that are not otherwise possible in the real world due to shame, social stigma, or risk of detection. As a consequence, there are now myriad opportunities for wrongdoing and abuse through technology. This book offers a comprehensive and integrative introduction to cybercrime. It is the first to connect the disparate literature on the various types of cybercrime, the investigation and detection of cybercrime and

the role of digital information, and the wider role of technology as a facilitator for social relationships between deviants and criminals. It includes coverage of: key theoretical and methodological perspectives, computer hacking and digital piracy, economic crime and online fraud, pornography and online sex crime, cyber-bulling and cyber-stalking, cyber-terrorism and extremism, digital forensic investigation and its legal context, cybercrime policy. This book includes lively and engaging features, such as discussion questions, boxed examples of unique events and key figures in offending, quotes from interviews with active offenders and a full glossary of terms. It is supplemented by a companion website that includes further students exercises and instructor resources. This text is essential reading for courses on cybercrime, cyber-deviancy, digital forensics, cybercrime investigation and the sociology of technology.

This book provides an account of the origins of transnational criminal law. The volume examines a range of topics, beginning with normative, intellectual, and institutional histories. It discusses specific transnational crimes ranging from piracy to cybercrime, and scrutinises jurisdiction, modes of liability, and the place of the individual.

The Government published the UK Cyber Security Strategy in June 2009 (Cm. 7642, ISBN 97801017674223), and established the Office of Cyber Security to provide strategic leadership across Government. This document sets out the Home Office's approach to tackling cyber crime, showing how to tackle such crimes directly through the provision of a law enforcement response, and indirectly through cross-Government working and through the development of relationships with industry, charities and other groups, as well as internationally. The publication is divided into five chapters and looks at the following areas, including: the broader cyber security context; cyber crime: the current position; the Government response and how the Home Office will tackle cyber crime.

The Law of Cybercrimes and Their Investigations

Cyber Criminals on Trial

Cybercrime in Context

Advancing the Service Sector with Evolving Technologies: Techniques and Principles

Internet Child Pornography and the Law

Principles of Cybercrime

This handbook explores organized crime, which it divides into two main concepts and types: the first is a set of stable organizations illegal per se or whose members systematically engage in crime, and the second is a set of serious criminal activities that are typically carried out for monetary gain.

"This book discusses the application of information systems to service creation, modeling, and evolution, covering foundational concepts and innovations in service management, service-oriented computing, strategic information systems, and Web services"--Provided by publisher.

Cyber Crimes against Women in India reveals loopholes in the present laws and policies of the Indian judicial system, and what can be done to ensure safety in cyberspace. The book is a

significant contribution to socio-legal research on online crimes targeting teenage girls and women. It shows how they become soft targets of trolling, online grooming, privacy infringement, bullying, pornography, sexual defamation, morphing, spoofing and so on. The authors address various raging debates in the country such as how women can be protected from cybercrimes; what steps can be taken as prevention and as recourse to legal aid and how useful and accessible cyber laws are. The book provides detailed answers to a wide array of questions that bother scholars and charts a way forward.

As computer-related crime becomes more important globally, both scholarly and journalistic accounts tend to focus on the ways in which the crime has been committed and how it could have been prevented. Very little has been written about what follows: the capture, possible extradition, prosecution, sentencing and incarceration of the cyber criminal. Originally published in 2004, this book provides an international study of the manner in which cyber criminals are dealt with by the judicial process. It is a sequel to the groundbreaking Electronic Theft: Unlawful Acquisition in Cyberspace by Grabosky, Smith and Dempsey (Cambridge University Press, 2001). Some of the most prominent cases from around the world are presented in an attempt to discern trends in the handling of cases, and common factors and problems that emerge during the processes of prosecution, trial and sentencing.

Cyber Victimology

International Approaches

Canadian Criminal Justice Today

Computer Crimes, Laws, and Policing in the 21st Century

Crime and Technology

Theory and prevention of technology-enabled offenses

This book provides a critical assessment of the problem of internet child pornography and its governance through legal and non-legal means, including a comparative assessment of laws in England and Wales, the United States of America and Canada in recognition that governments have a compelling interest to protect children from sexual abuse and exploitation. The internet raises novel and complex challenges to existing regulatory regimes. Efforts towards legal harmonization at the European Union, Council of Europe, and United Nations level are examined in this context and the utility of additional and alternative

methods of regulation explored. This book argues that effective implementation, enforcement and harmonization of laws could substantially help to reduce the availability and dissemination of child pornography on the internet. At the same time, panic-led policies must be avoided if the wider problems of child sexual abuse and commercial sexual exploitation are to be meaningfully addressed.

A comprehensive doctrinal analysis of cybercrime laws in four major common law jurisdictions: Australia, Canada, the UK and the USA.

"Digital Evidence and Computer Crime" provides the knowledge necessary to uncover and use digital evidence effectively in any kind of investigation. This completely updated edition provides the introductory materials that new students require, and also expands on the material presented in previous editions to help students develop these skills.

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.

Cyber Crime and the Victimization of Women

Cybercrime

Histories of Transnational Criminal Law

The American System of Criminal Justice

Cyber crime strategy

New Frontiers for Regulation, Law Enforcement and Research

Guido Rossi As Chairman of ISPAC, I want to thank all the contributors to this book that originates from the International Conference on Crime and Technology. This could be the end of my presentation if I did not feel uneasy not considering one of the problems I believe to be pivotal in the relationship between crime and technology. I shall also consider that the same relationship exists between terror and globalization, while globalization is stemming from technology and terror from crime. Transnational terrorism is today made possible by the vast array of communication tools. But the paradox is that if globalization facilitates terrorist violence, the fight against this war without borders is potentially disastrous for both economic development and globalization. Antiterrorist measures restrict mobility and financial flows, while new terrorist attacks could lead the way for an antiglobalist reaction. But the global society has yet to agree on a common definition of terrorism or on a common policy against it. The ordinary traditional criminal law is still depending on the sovereignty of national states, while international criminal justice is only a spotty and contested last resort. The fragmented and weak international institutions and underdeveloped civil societies have no power to enforce criminal justice against t- rorism. At the same time, the states that are its targets have no interest in applying the laws of war (the Geneva Conventions) to their fight against terrorists.

This collection is innovative and original. It introduces new knowledge and is very timely because of the current high profile of the international public discourse over security, the internet and its impact upon the growth of the information economy. The book will be very useful to a wide range of readers because it will both inform and provide the basis for instruction. This book significantly advances the scholarly literature available on the global problem of cyber-crime. It also makes a unique contribution to the literature in this area. Much of what has been written focuses on cyber-crime in the United States and in Europe. This much-needed volume focuses on how cyber-crime is being dealt with in Asian countries. It explains how law enforcement is responding to the complex issues cyber-crime raises and analyzes the difficult policy issues this new type of transnational crime

generates. This book is an invaluable addition to the library of anyone who is concerned about online crime, computer security or the emerging culture of the Internet.

This book is about the human factor in cybercrime: its offenders, victims and parties involved in tackling cybercrime. It takes a diverse international perspective of the response to and prevention of cybercrime by seeking to understand not just the technological, but the human decision-making involved. This edited volume represents the state of the art of research on the human factor in cybercrime, addressing its victims, offenders, and policing. It originated at the Second annual Conference on the Human Factor in Cybercrime, held in The Netherlands in October 2019, bringing together empirical research from a variety of disciplines, and theoretical and methodological approaches. This volume will be of particular interest to researchers and students in cybercrime and the psychology of cybercrime, as well as policy makers and law enforcement interested in prevention and detection.

Cybercrime in Canadian Criminal LawCarswell Legal Publications

Digital Criminology

Scene of the Cybercrime

Transnational Criminal Organizations, Cybercrime, and Money Laundering

Techniques and Principles

International Guide to Combating Cybercrime

Corporate Hacking and Technology-driven Crime

The third edition of this book presents the history of computer crime and cybercrime from the very beginning with punch cards, to the latest developments - including the attacks in the context of the 2016 US Election. Today the technological development of social media, such as Google, Facebook, YouTube, Twitter, and more, have been so rapid and the impact on society so fast and enormous, that codes of ethics, and public sentiments of justice implemented in criminal legislations, have not kept pace. Conducts in social media need a better protection by criminal laws. The United Nations Declarations and principles for the protection of individual and human rights are fundamental rights also in Cyberspace. The same rights that people have offline must also be protected online. Cyber attacks against critical information infrastructures of sovereign States, public institutions, private industry and individuals, must necessitate a response for global solutions. In conducting investigation and prosecution of cybercrime countries should understand that international coordination and cooperation are necessary in prosecuting cross-border cybercrime. It is critical that the police work closely with government and other elements of the criminal justice system, Interpol, Europol and other international organizations.

The emergence of the World Wide Web, smartphones, and computers has transformed the world and enabled individuals to engage in crimes in a multitude of new ways. Criminological scholarship on these issues has increased dramatically over the last decade, as have studies on ways to prevent and police these offenses. This book is one of the first texts to provide a comprehensive review of research regarding cybercrime, policing and enforcing these offenses, and the prevention of various offenses as global change and technology adoption increases the risk of victimization around the world. Drawing on a wide range of literature, Holt and Bossler offer an extensive synthesis of numerous contemporary topics such as theories used to account for cybercrime, policing in domestic and transnational contexts, cybercrime victimization and issues in cybercrime prevention. The findings provide a roadmap for future research in cybercrime, policing, and technology, and discuss key controversies in the existing research literature in a way that is otherwise absent from textbooks and general cybercrime readers. This

book is an invaluable resource for academics, practitioners, and students interested in understanding the state of the art in social science research. It will be of particular interest to scholars and students interested in cybercrime, cyber-deviance, victimization, policing, criminological theory, and technology in general.
"Cybercrime in Canadian Criminal Law is a treatise on computer crime for the Canadian marketplace. It provides concrete answers to the difficult question of how to successfully deal with computer crime in Canada. It sets out the existing regulatory framework and considers alternatives in depth. It also provides a complex, multi-tiered proposal for effective law enforcement, while considering the question of constitutional and other constraints on regulation, including cost. It also draws analogies to existing law enforcement powers in other areas, such as terrorism and money laundering, as well as related technologies, including telephone networks. Finally, it discusses how similar measures have been implemented in other jurisdictions throughout the world."--Pub. desc.
States criminalize a wide range of transnational offences, such as piracy, human trafficking, drug trafficking, terrorism, organized crime, and cybercrime. This book provides an introduction to this developing area of law, setting out what transnational crimes are, and how states can establish jurisdiction over them and enforce it.
Cybercrime and Digital Forensics
Cybercrime, Organized Crime, and Societal Responses
An Introduction to Transnational Criminal Law
A Handbook for Law Enforcement Officers, Auditors, and Financial Investigators
Forensic Science, Computers and the Internet
An Introductory Text for the Twenty-first Century
WRITTEN BY A LAW ENFORCEMENT PROFESSIONAL FOR OTHER LAW ENFORCEMENT PERSONNEL IN THE TRENCHES This book examines the workings of organized criminals and criminal groups that transcend national boundaries. Discussions include methods used by criminal groups to internationally launder money; law enforcement efforts to counteract such schemes; and new methods and tactics to counteract transnational money laundering. A PRACTICAL GUIDE TO FACETS OF INTERNATIONAL CRIME AND MEASURES TO COMBAT THEM Intended for law enforcement personnel, bank compliance officers, financial investigators, criminal defense attorneys, and anyone interested in learning about the basic concepts of international crime and money laundering, this timely text explains: money laundering terms and phrases an overview of relevant federal agencies, transnational criminal organizations, and basic investigatory techniques the intricacies of wire transfers and cyberbanking the phenomenon of the "World Wide Web"
"Cybercrime in Canadian Criminal Law is a treatise on computer crime for the student and practitioner alike. It provides concrete answers to the difficult question of how to successfully deal with computer crime in Canada. It sets out the existing regulatory framework and considers alternatives in depth. It also provides a complex, multi-tiered proposal for effective law enforcement, while considering the question of constitutional and other constraints on regulation, including cost. In addition, it draws analogies to existing law enforcement powers in other areas, such as terrorism and money laundering, as well as related technologies, including telephone networks. Finally, it discusses how similar measures have been implemented in other jurisdictions throughout the world." --Pub. desc.

Providing an introduction to, and detailed examination of substantive, enforcement and procedural aspects of international criminal law, this book's examination of international and transnational crimes under treaty and customary law has been fully updated and revised. Exploring the enforcement of international criminal law through an investigation of the practice of the Security Council-based tribunals for Yugoslavia and Rwanda, the International Criminal Court and other hybrid tribunals, such as those for Cambodia, Sierra Leone, Lockerbie and truth commissions, the authors look at terrorism, offences against the person, piracy and jurisdiction, and immunities amongst a variety of other topics. New to this edition are four additional chapters on: various forms of liability and participation in international crime war crimes crimes against humanity genocide and illegal rendition. This is an ideal text for undergraduate and postgraduate students of law or international relations, practitioners and those interested in gaining an insight into international criminal law

Cyber Victimology provides a global socio-legal-victimological perspective on victimisation online, written in clear, non-technical terms, and presents practical solutions for the problem. Halder qualitatively analyses the contemporary dimensions of cyber-crime victimisation, aiming to fill the gap in the existing literature on this topic. A literature review, along with case studies, allows the author to analyse the current situation concerning cyber-crime victimisation. A profile of victims of cyber-crime has been developed based on the characteristics of different groups of victims. As well, new policy guidelines on the basis of UN documents on cybercrimes and victim justice are proposed to prevent such victimisation and to explore avenues for restitution of justice for cases of cyber-crime victimisation. This book shows how the effects of cyber victimisation in one sector can affect others. This book also examines why perpetrators choose to attack their victim/s in specific ways, which then have a ripple effect, creating greater harm to other members of society in unexpected ways. This book is suitable for use as a textbook in cyber victimology courses and will also be of great interest to policy makers and activists working in this area.

The human factor in victimization, offending, and policing

An Introduction

Understanding Cybersecurity Law and Digital Privacy

Digital Evidence and Computer Crime

The Challenge in Asia

This classic best seller, commonly referred to as The Eagle, helps students discover the challenges of pursuing justice in our society and identify the roles individuals play in the criminal justice system. Using an interdisciplinary lens, THE AMERICAN SYSTEM OF CRIMINAL JUSTICE, 16th Edition, presents elements from criminology, sociology, law, history, psychology, and political science. This approach challenges students to ask important questions and recognize contemporary problems as the means to build their understanding of the system's components and stages as well as its human consequences and policy challenges. Cole, Smith, and

DeJong offer solid scholarship, approachable writing, and current, compelling events and cases that hold students' attention, thereby preparing them to participate in the system as citizens and future criminal justice practitioners. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Cybercrime has become increasingly prevalent in the new millennium as computer-savvy criminals have developed more sophisticated ways to victimize people online and through other digital means. The Law of Cybercrimes and Their Investigations is a comprehensive text exploring the gamut of issues surrounding this growing phenomenon. After an introduction to the history of computer crime, the book reviews a host of topics including: Information warfare and cyberterrorism Obscenity, child pornography, sexual predator conduct, and online gambling Cyberstalking, cyberharassment, cyberbullying, and other types of unlawful expression Auction fraud, Ponzi and pyramid schemes, access device fraud, identity theft and fraud, securities and bank fraud, money laundering, and electronic transfer fraud Data privacy crimes, economic espionage, and intellectual property crimes Principles applicable to searches and seizures of computers, other digital devices, and peripherals Laws governing eavesdropping, wiretaps, and other investigatory devices The admission of digital evidence in court Procedures for investigating cybercrime beyond the borders of the prosecuting jurisdiction Each chapter includes key words or phrases readers should be familiar with before moving on to the next chapter. Review problems are supplied to test assimilation of the material, and the book contains weblinks to encourage further study.

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.

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.

A Common Law Perspective

Methodologies, Ethics, and Critical Approaches

National and International Responses

Internet and Distributed Computing Advancements: Theoretical Frameworks and Practical Applications

Cyber-Crime

The Transformation of Crime in the Information Age

Digital technology is ever-changing, which means that those working or planning to work in IT or apply IT systems must strategize how and what applications and technologies are ideal for sustainable civilization and human development. Developmental trends of IT and the digitalization of enterprise, agriculture, healthcare, education, and more must be explored within the boundaries of ethics and law in order to ensure that IT does not have a harmful effect on society. The Strategies of Informing Technology in the 21st Century is a critical authored reference book that develops the strategic attitude in developing and operating IT applications based on the requirements of sustainable civilization and ethical and wise applications of technology in society. Technological progress is examined including trends in automation, artificial intelligence, and information systems. The book also specifically covers applications of digital informing strategies in business, healthcare, agriculture, education, and the home. Covering key concepts such as automation, robotization, and digital infrastructure, it is ideal for IT executives, CIS/MIS/CS faculty, cyber ethics professionals, technologists, systems engineers, IT specialists and consultants, security analysts, students, researchers, and academicians.

When it comes to computer crimes, the criminals got a big head start. But the law enforcement and IT security communities are now working diligently to develop the knowledge, skills, and tools to successfully investigate and prosecute Cybercrime cases. When the first edition of "Scene of the Cybercrime" published in 2002, it was one of the first books that educated IT security professionals and law enforcement how to fight Cybercrime. Over the past 5 years a great deal has changed in how computer crimes are perpetrated and subsequently investigated. Also, the IT security and law enforcement communities have dramatically improved their ability to deal with Cybercrime, largely as a result of increased spending and training. According to the 2006 Computer Security Institute's and FBI's joint Cybercrime report: 52% of companies reported unauthorized use of computer systems in the prior 12 months. Each of these incidents is a Cybecrime requiring a certain level of investigation and remediation. And in many cases, an investigation is mandates by federal compliance regulations such as Sarbanes-Oxley, HIPAA, or the Payment Card Industry (PCI) Data Security Standard. Scene of the Cybercrime, Second Edition is a completely revised and updated book which covers all of the technological, legal, and regulatory changes, which have occurred since the first edition. The book is written for dual audience; IT

security professionals and members of law enforcement. It gives the technical experts a little peek into the law enforcement world, a highly structured environment where the "letter of the law" is paramount and procedures must be followed closely lest an investigation be contaminated and all the evidence collected rendered useless. It also provides law enforcement officers with an idea of some of the technical aspects of how cyber crimes are committed, and how technology can be used to track down and build a case against the criminals who commit them. Scene of the Cybercrime, Second Editions provides a roadmap that those on both sides of the table can use to navigate the legal and technical landscape to understand, prevent, detect, and successfully prosecute the criminal behavior that is as much a threat to the online community as "traditional" crime is to the neighborhoods in which we live. Also included is an all new chapter on Worldwide Forensics Acts and Laws. * Companion Web site provides custom tools and scripts, which readers can download for conducting digital, forensic investigations. * Special chapters outline how Cybercrime investigations must be reported and investigated by corporate IT staff to meet federal mandates from Sarbanes Oxley, and the Payment Card Industry (PCI) Data Security Standard * Details forensic investigative techniques for the most common operating systems (Windows, Linux and UNIX) as well as cutting edge devices including iPods, Blackberries, and cell phones.

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.

Cybercrime in Canadian Criminal Law

Interpersonal Criminology

Revisiting Interpersonal Crimes and Victimization

The History of Cybercrime

Decoding Cyber Crime Victimization