Privacy On The Line The Politics Of Wiretapping

Through critical analysis of case law in European and national courts, this book reveals the significant role courts play in the protection of privacy and personal data within the new technological environment. It addresses the pressing question from a public who are increasingly aware of their privacy rights in a world of continual technological advances – namely, what can I do if my data privacy rights are breached?

The wide gap between the existing security solutions and the actual practical deployment in smart manufacturing, smart home, and remote environments (with respect to wireless robotics) is one of the major reasons why we require novel strategies, mechanisms, architectures, and frameworks. Furthermore, it is also important to access and understand the different level of vulnerabilities and attack vectors in Wireless Sensor Network (WSN) and Wireless Robotics. This book includes an in-depth explanation of a secure and dependable Wireless Robotics (WR) architecture, to ensure confidentiality, authenticity, and availability. Features Blockchain technology for securing data at end/server side Emerging technologies/networking, like Cloud, Edge, Fog, etc., for communicating and storing data (securely). Various open issues, challenges faced in this era towards wireless robotics, including several future research directions for the future. Several real world's case studies are included Chapters on ethical concerns and privacy laws, i.e., laws for service providers Security and privacy challenges in wireless sensor networks and wireless robotics The book is especially useful for academic researchers, undergraduate students, postgraduate students, and industry researchers and professionals.

A penetrating and insightful study of privacy and security in telecommunications for a post-9/11, post-Patriot Act world. Telecommunication has never been perfectly secure. The Cold War culture of recording devices in telephone receivers and bugged embassy offices has been succeeded by a post-9/11 world of NSA wiretaps and demands for data retention. Although the 1990s battle for individual and commercial freedom to use cryptography was won, growth in the use of cryptography has been slow. Meanwhile, regulations requiring that the computer and communication industries build spying into their systems for government convenience have increased rapidly. The application of the 1994 Communications Assistance for Law Enforcement Act has expanded beyond the intent of Congress to apply to voice over Internet Protocol (VoIP) and other modern data services; attempts are being made to require ISPs to retain their data for years in case the government wants it; and data mining techniques developed for commercial marketing applications are being applied to widespread surveillance of the population. In Privacy on the Line, Whitfield Diffie and Susan Landau strip away the hype surrounding the policy debate over privacy to examine the national security, law enforcement, commercial, and civil liberties issues. They discuss the social function of privacy, how it underlies a democratic society, and what happens when it is lost. This updated and expanded edition revises their original -- and prescient -- discussions of both policy and technology in light of recent controversies over NSA spying and other government threats to communications privacy.

A penetrating and insightful study of privacy and security in telecommunications for a post-9/11, post-Patriot Act world. Telecommunication has never been perfectly secure. The Cold War culture of recording devices in telephone receivers and bugged embassy offices has been succeeded by a post-9/11 world of NSA wiretaps and demands for data retention. Although the 1990s battle for individual and commercial freedom to use cryptography was won, growth in the use of cryptography has been slow. Meanwhile, regulations requiring that the computer and communication industries build spying into their systems for government convenience have increased rapidly. The application of the 1994 Communications Assistance for Law Enforcement Act has expanded beyond the intent of Congress to apply to voice over Internet Protocol (VoIP) and other modern data services; attempts are being made to require ISPs to retain their data for years in case the government wants it; and data mining techniques developed for commercial marketing applications are being applied to widespread surveillance of the population. In Privacy on the Line, Whitfield Diffie and Susan Landau strip away the hype surrounding the policy debate over privacy to examine the national security, law enforcement, commercial, and civil liberties issues. They discuss the social function of privacy, how it underlies a democratic society, and what happens when it is lost. This updated and expanded edition revises their original—and prescient—discussions of both policy and technology in light of recent controversies over NSA spying and other government threats to communications privacy.

Hearing Before the Committee on Commerce, Science, and Transportation, United States Senate, One Hundred Eighth Congress, First Session, September 17, 2003

Ben Franklin's Web Site

Federal Agency Protection of Privacy Act of 2004

The Oxford Handbook of Internet Studies

Courts, Privacy and Data Protection in the Digital Environment

Title Privacy and Data Protection based on the GDPR

1999 IEEE-USAB Award for Distinguished Literary Contributions Furthering Public Understanding of the Profession. and Winner of the 1998 Donald McGannon Award for Social and Ethical Relevance in Communication Policy Research Telecommunication has never been perfectly secure, as a Cold War culture of wiretaps and international spying taught us. Yet many of us still take our privacy for granted, even as we become more reliant than ever on telephones, computer networks, and electronic transactions of all kinds. Whitfield Diffie and Susan Landau argue that if we are to retain the privacy that characterized face-to-face relationships in the past, we must build the means of protecting that privacy into our communication systems. Diffie and Landau strip away the hype surrounding the policy debate to examine the national security, law enforcement, commercial, and civil liberties issues. They discuss the social function of privacy, how it underlies a democratic society, and what happens when it is lost.

The idea of a right to privacy, which arose in reaction to the rapid rise of newspapers, instant photography and the "paparazzi" of the 19th century, has evolved into a constitutional right in much of the developed world. It is enshrined in Hong Kong through Articles 28, 29, 30 and 39 of the Basic Law. Hong Kong stands proud as the first jurisdiction in Asia to enact legislation to safeguard personal data in the form of the Personal Data (Privacy) Ordinance, Cap 486 ("the Ordinance") which came into force in 1996. At its centre are the six Data Protection Principles based on the 1980 OECD

Guidelines. The office of the Privacy Commissioner for Personal Data was created under this legislation to provide oversight and ensure compliance. The Octopus scandal in mid-2010 eventually led to substantial changes being made to the Ordinance that were enacted in 2012 and 2013, the main amendments being the Direct Marketing provisions and the provision of legal assistance and representation to aggrieved persons. In this digital age, the Ordinance is proving to be the main safeguard of our privacy rights. The Data Protection Principles seek to create broad common principles based on fairness that apply to the public and private sectors. The passage of twenty years since the enactment of the Ordinance has given rise to a substantial body of case law and administrative decisions on these principles and the other provisions of the Ordinance. The new amendments have already been the subject of judicial scrutiny. This publication, which replaces its predecessor, has the dual aim of becoming a practitioner ' s guide on the important subject of personal data privacy, containing, as it does, a detailed exposition of the principles and provisions in the Ordinance and a comprehensive source of reference materials, and of enabling the Privacy Commissioner to discharge his major duty to promote awareness and understanding of the Ordinance. The second edition includes not only a full discussion of these principles, but also summaries of all the seminal cases and Administrative Appeals Board rulings in this area, as well as a comprehensive list of all the pertinent cases.

This book constitutes the refereed proceedings of the 36th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy, DBSec 2022, held in Newark, NJ, USA, in July 2022. The 12 full papers and 6 short papers presented were carefully reviewed and selected from 33 submissions. The conference covers research in data and applications security and privacy.

Recoge: Part one: 1. Description of the general situation -- 2. Technical on line network operators -- 3. Overview of on line services and the protection of privacy -- Part two: 1. Case studies -- 2. "Rep Agency" NYTEMC.America on line. The 2nd World.Fnac Direct.

Privacy Handbook

Security, Privacy and Trust in the IoT Environment

A Novel

Data and Applications Security and Privacy XXXVI

On-line Services and Data Protection and the Protection of Privacy

Legal and Privacy Issues in Information Security

Focuses on the possibility of creating serious security risks by housing wiretapping within communication infrastructure and whether widespread communications surveillance enhances or endangers national security. Landau explains that understanding whether building wiretapping into communication infrastructure keeps us safe requires that we understand the technology, economics, law, and policy issues of communication surveillance technologies. She offers a set of principles to govern wiretapping policy that will allow us to protect our national security as well as our freedom.

Mobile internet data has the characteristics of large scale, variety of patterns, and complex association. On the one hand, it needs an efficient data processing model to provide support for data services, and, on the other hand, it needs certain computing resources to provide data security services. Due to the limited resources of mobile terminals, it is impossible to complete large-scale data computation and storage. However, outsourcing to third parties may cause risks in user privacy protection. This monograph focuses on key technologies of data service outsourcing and privacy protection, including the existing methods of data analysis and processing, fine-grained data access control through effective user privacy protection mechanisms, and data sharing in the mobile internet.

Internet Studies has been one of the most dynamic and rapidly expanding interdisciplinary fields to emerge over the last decade. The Oxford Handbook of Internet Studies has been designed to provide a valuable resource for academics and students in this area, bringing together leading scholarly perspectives on how the Internet has been studied and how the research agenda should be pursued in the future. The Handbook aims to focus on Internet Studies as an emerging field, each chapter seeking to provide a synthesis and critical assessment of the research in a particular area. Topics covered include social perspectives on the technology of the Internet, its role in everyday life and work, implications for communication, power, and influence, and the governance and regulation of the Internet. The Handbook is a landmark in this new interdisciplinary field, not only helping to strengthen research on the key questions, but also shape research, policy, and practice across many disciplines that are finding the Internet and its political, economic, cultural, and other societal implications increasingly central to their own key areas of inquiry.

Most people believe that the right to privacy is inherently at odds with the right to free speech. Courts all over the world have struggled with how to reconcile the problems of media gossip with our commitment to free and open public debate for over a century. The rise of the Internet has made this problem more urgent. We live in an age of corporate and government surveillance of our lives. And our free speech culture has

created an anything-goes environment on the web, where offensive and hurtful speech about others is rife. How should we think about the problems of privacy and free speech? In Intellectual Privacy, Neil Richards offers a different solution, one that ensures that our ideas and values keep pace with our technologies. Because of the importance of free speech to free and open societies, he argues that when privacy and free speech truly conflict, free speech should almost always win. Only when disclosures of truly horrible information are made (such as sex tapes) should privacy be able to trump our commitment to free expression. But in sharp contrast to conventional wisdom, Richards argues that speech and privacy are only rarely in conflict. America's obsession with celebrity culture has blinded us to more important aspects of how privacy and speech fit together. Celebrity gossip might be a price we pay for a free press, but the privacy of ordinary people need not be. True invasions of privacy like peeping toms or electronic surveillance will rarely merit protection as free speech. And critically, Richards shows how most of the law we enact to protect online privacy pose no serious burden to public debate, and how protecting the privacy of our data is not censorship. More fundamentally, Richards shows how privacy and free speech are often essential to each other. He explains the importance of 'intellectual privacy,' protection from surveillance or interference when we are engaged in the processes of generating ideas - thinking, reading, and speaking with confidantes before our ideas are ready for public consumption. In our digital age, in which we increasingly communicate, read, and think with the help of technologies that track us, increased protection for intellectual privacy has become an imperative. What we must do, then, is to worry less about barring tabloid gossip, and worry much more about corporate and government surveillance into the minds, conversations, reading habits, and political beliefs of ordinary people. A timely and provocative book on a subject that affects us all, Intellectual Privacy will radically reshape the debate about privacy and free speech in our digital age.

Network-on-Chip Security and Privacy

On-line Services and Data Protection and the Protection of Privacy: Description of the general situation. Case studies

Guidelines, Exposures, Policy Implementation, and International Issues

Big Data Is Not a Monolith

The USA, Mass Surveillance and the Spiral Model

We don't have to tell you that keeping up with privacy guidelines and having a strong privacy policy are critical in today's network economy. More and more organizations are instating the position of a Corporate Privacy Officer (CPO) to oversee all of the privacy issues within and organization. The Corporate Privacy Handbook will provide you with a comprehensive reference on privacy guidelines and instruction on policy development/implementation to guide corporations in establishing a strong privacy policy. Order your copy today!

Perspectives on the varied challenges posed by big data for health, science, law, commerce, and politics. Big data is ubiquitous but heterogeneous. Big data can be used to tally clicks and traffic on web pages, find patterns in stock trades, track consumer preferences, identify linguistic correlations in large corpuses of texts. This book examines big data not as an undifferentiated whole but contextually, investigating the varied challenges posed by big data for health, science, law, commerce, and politics. Taken together, the chapters reveal a complex set of problems, practices, and policies. The advent of big data methodologies has challenged the theory-driven approach to scientific knowledge in favor of a data-driven one. Social media platforms and self-tracking tools change the way we see ourselves and others. The collection of data by corporations and government threatens privacy while promoting transparency. Meanwhile, politicians, policy makers, and ethicists are ill-prepared to deal with big data's ramifications. The contributors look at big data's effect on individuals as it exerts social control through monitoring, mining, and manipulation; big data and society, examining both its empowering and its constraining effects; big data and science, considering issues of data governance, provenance, reuse, and trust; and big data and organizations, discussing data responsibility, “data harm,” and decision making. Contributors Ryan Abbott, Cristina Alaimo, Kent R. Anderson, Mark Andrejevic, Diane E. Bailey, Mike Bailey, Mark Burdon, Fred H. Cate, Jorge L. Contreras, Simon DeDeo, Hamid R. Ekbia, Allison Goodwell, Jannis Kallinikos, Inna Kouper, M. Lynne Markus, Michael Mattioli, Paul Ohm, Scott Peppet, Beth Plale, Jason Portenoy, Julie Rennecker, Katie Shilton, Dan Sholler, Cassidy R. Sugimoto, Isuru Suriarachchi, Jevin D. West

This book constitutes the refereed proceedings of the 27th IFIP WG 11.3 International Conference on Data and Applications Security and Privacy, DBSec 2013, held in Newark, NJ,

USA in July 2013. The 16 revised full and 6 short papers presented were carefully reviewed and selected from 45 submissions. The papers are organized in topical sections on privacy, access control, cloud computing, data outsourcing, and mobile computing.
This two-volume set LNICST 398 and 399 constitutes the post-conference proceedings of the 17th International Conference on Security and Privacy in Communication Networks, SecureComm 2021, held in September 2021. Due to COVID-19 pandemic the conference was held virtually. The 56 full papers were carefully reviewed and selected from 143 submissions. The papers focus on the latest scientific research results in security and privacy in wired, mobile, hybrid and ad hoc networks, in IoT technologies, in cyber-physical systems, in next-generation communication systems in web and systems security and in pervasive and ubiquitous computing.
Personal Data (Privacy) Law in Hong Kong A Practical Guide on Compliance (Second Edition)
Citizens' Perspectives
Surveillance, Privacy and Security
Web Security, Privacy & Commerce
27th Annual IFIP WG 11.3 Conference, DBSec 2013, Newark, NJ, USA, July 15-17, 2013, Proceedings
Report (to Accompany H.R. 338) (including Cost Estimate of the Congressional Budget Office).

"Web Security, Privacy & Commerce" cuts through the hype and the front page stories. It tells readers what the real risks are and explains how to minimize them. Whether a casual (but concerned) Web surfer or a system administrator responsible for the security of a critical Web server, this book will tells users what they need to know.

This volume examines the relationship between privacy, surveillance and security, and the alleged privacy–security trade-off, focusing on the citizen's perspective. Recent revelations of mass surveillance programmes clearly demonstrate the ever-increasing capabilities of surveillance technologies. The lack of serious reactions to these activities shows that the political will to implement them appears to be an unbroken trend. The resulting move into a surveillance society is, however, contested for many reasons. Are the resulting infringements of privacy and other human rights compatible with democratic societies? Is security necessarily depending on surveillance? Are there alternative ways to frame security? Is it possible to gain in security by giving up civil liberties, or is it even necessary to do so, and do citizens adopt this trade-off? This volume contributes to a better and deeper understanding of the relation between privacy, surveillance and security, comprising in-depth investigations and studies of the common narrative that more security can only come at the expense of sacrifice of privacy. The book combines theoretical research with a wide range of empirical studies focusing on the citizen's perspective. It presents empirical research exploring factors and criteria relevant for the assessment of surveillance technologies. The book also deals with the governance of surveillance technologies. New approaches and instruments for the regulation of security technologies and measures are presented, and recommendations for security policies in line with ethics and fundamental rights are discussed. This book will be of much interest to students of surveillance studies, critical security studies, intelligence studies, EU politics and IR in general. A PDF version of this book is available for free in open access via www.tandfebooks.com. It has been made available under a Creative Commons Attribution-Non Commercial 3.0 license.

This book provides a thorough treatment of privacy and security issues for researchers in the fields of smart grids, engineering, and computer science. It presents comprehensive insight to understanding the big picture of privacy and security challenges in both physical and information aspects of smart grids. The authors utilize an advanced interdisciplinary approach to address the existing security and privacy issues and propose legitimate countermeasures for each of them in the standpoint of both computing and electrical engineering. The proposed methods are theoretically proofed by mathematical tools and illustrated by real-world examples.

This book aims to explain the US violation of the human right to privacy unveiled by Edward Snowden with a newly developed comprehensive spiral model. After analyzing the social and juridical roots of the norm of privacy, it portrays the countering of privacy by the security norm in the US public debate and the US policy from the 1930s to 2013. On the basis of this case study the author refines the spiral model invented by Risse et al. Finally, the book explores the reaction of several actors following the Snowden disclosures and analyzes the tools these actors have used to influence the behavior of the USA. Thereby the author examines if the US reactions to the Snowden disclosures since 2013 follow the heuristic approach o

Security and Privacy in Communication Networks
Security and Privacy-Preserving Techniques in Wireless Robotics
Description of the general situation. Case studies
Data and Applications Security and Privacy XXVII
On-line Services and Data Protection and Privacy
The Abolishment of the Right to Privacy?

This book addresses the privacy issue of On-Line Analytic Processing (OLAP) systems. OLAP systems usually need to meet two conflicting goals. First, the sensitive data stored in underlying data warehouses must be kept secret. Second, analytical queries about the data must be allowed for decision support purposes. The main challenge is that sensitive data can be inferred from answers to seemingly innocent aggregations of the data. This volume reviews a series of methods that can precisely answer data cube-style OLAP, regarding sensitive data while provably preventing adversaries from inferring data.
Security and privacy protection within computer networks can be a challenge. By examining the current

problems and challenges this domain is facing, more efficient strategies can be established to safeguard personal information against invasive pressures. Security and Privacy in Smart Sensor Networks is a critical scholarly resource that examines recent developments and emerging trends in smart sensor security and privacy by providing new models, practical solutions, and technological advances related to security. Featuring coverage on a broad range of topics such as cloud security, encryption, and intrusion detection systems, this book is geared towards academicians, engineers, IT specialists, researchers, and students seeking current research on authentication and intrusion detection.

The Internet of Things (IoT) is a network of devices and smart things that provides a pervasive environment in which people can interact with both the cyber and physical worlds. As the number and variety of connected objects continue to grow and the devices themselves become smarter, users' expectations in terms of adaptive and self-governing digital environments are also on the rise. Although, this connectivity and the resultant smarter living is highly attractive to general public and profitable for the industry, there are also inherent concerns. The most challenging of these refer to the privacy and security of data, user trust of the digital systems, and relevant authentication mechanisms. These aspects call for novel network architectures and middleware platforms based on new communication technologies; as well as the adoption of novel context-aware management approaches and more efficient tools and devices. In this context, this book explores central issues of privacy, security and trust with regard to the IoT environments, as well as technical solutions to help address them. The main topics covered include: Basic concepts, principles and related technologies Security/privacy of data, and trust issues Mechanisms for security, privacy, trust and authentication Success indicators, performance metrics and future directions. This reference text is aimed at supporting a number of potential audiences, including Network Specialists, Hardware Engineers and Security Experts Students, Researchers, Academics and Practitioners.

This book provides comprehensive coverage of Network-on-Chip (NoC) security vulnerabilities and state-of-the-art countermeasures, with contributions from System-on-Chip (SoC) designers, academic researchers and hardware security experts. Readers will gain a clear understanding of the existing security solutions for on-chip communication architectures and how they can be utilized effectively to design secure and trustworthy systems.

36th Annual IFIP WG 11.3 Conference, DBSec 2022, Newark, NJ, USA, July 18–20, 2022, Proceedings

The Politics of Wiretapping and Encryption

Hearings Before the Subcommittee on Telecommunications and Finance of the Committee on Energy and Commerce, House of Representatives, One Hundred Third Congress, First Session, May 25 and June 24, 1993

Rethinking Civil Liberties in the Digital Age

Right of Privacy Act of 1967

Smart Grids: Security and Privacy Issues

Thoroughly revised and updated to address the many changes in this evolving field, the third edition of Legal and Privacy Issues in Information Security addresses the complex relationship between the law and the practice of information security. Information systems security and legal compliance are required to protect critical governmental and corporate infrastructure, intellectual property created by individuals and organizations alike, and information that individuals believe should be protected from unreasonable intrusion. Organizations must build numerous information security and privacy responses into their daily operations to protect the business itself, fully meet legal requirements, and to meet the expectations of employees and customers. Instructor Materials for Legal Issues in Information Security include: PowerPoint Lecture Slides Instructor's Guide Sample Course Syllabus Quiz & Exam Questions Case Scenarios/Handouts New to the third Edition: • Includes discussions of amendments in several relevant federal and state laws and regulations since 2011 • Reviews relevant court decisions that have come to light since the publication of the first edition • Includes numerous information security data breaches highlighting new vulnerabilities

As Justice Louis Brandeis suggested more than a century ago, privacy--the right to be left alone--is the most valued, if not the most celebrated, right enjoyed by Americans. But in the face of computer, video, and audio technology, aggressive and sophisticated marketing databases, state and federal "wars" against crime and terrorism, new laws governing personal behavior, and an increasingly intrusive media, all of us find our personal space and freedom under attack. In The End of Privacy, Charles Sykes traces the roots of privacy in our nation's founding and Constitution, and reveals its inexorable erosion in our time. From our homes and offices to the presidency, Sykes defines what we have lost, citing example after example of citizens who have had their conversations monitored, movements surveilled, medical and financial records accessed, sexual preferences revealed, homes invaded, possessions confiscated, and even lives threatened--all in the name of some alleged higher social or governmental good. Sykes

concludes by suggesting steps by which we might begin to recover the territory we've lost: our fundamental right to our own lives.

Privacy on the LineThe Politics of Wiretapping and EncryptionMIT Press

Explore the hidden niches of American history to discover the tug between our yearning for privacy and our insatiable curiosity. Book jacket.

A Resource Document in Relation to Privacy in Telecommunications

Information Privacy Engineering and Privacy by Design

Telephone Privacy

Hearings, Ninetieth Congress, First Session, Pursuant to S. Res. 25, on S. 928

Privacy on the Line

Privacy on the Line, updated and expanded edition

Information about people is becoming increasingly valuable. Enabled by new technologies, organizations collect and process personal data on a large scale. Free flow of data across Europe is vital for the common market, but it also presents a clear risk to the fundamental rights of individuals. This issue was addressed by the Council of the European Union and the European Parliament with the introduction of the General Data Protection Regulation (GDPR). For many organizations processing personal data, the GDPR came as a shock. Not so much its publication in the spring of 2016, but rather the articles that appeared about it in professional journals and newspapers leading to protests and unrest. The heavy requirements of the law would cause very expensive measures in companies and organizations, was a concern. In addition, companies which failed to comply would face draconian fines. This book is intended to explain where these requirements came from and to prove that the GDPR is not incomprehensible, that the principles are indeed remarkably easy to understand. It will help anyone in charge of, or involved in, the processing of personal data to take advantage of the innovative technologies in processing without being unduly hindered by the limitations of the GDPR. The many examples and references to EDPB (European Data Protection Board) publications, recent news articles and case law clarify the requirements of the law and make them accessible and understandable. Leo's book can provide very effective support to you and your colleagues in reaching this understanding and applying it in practice. Fintan Swanton, Managing Director of Cygnus Consulting Ltd., Ireland.

In preparation for this book, and to better understand our screen-based, digital world, Miller only accessed information online for seven years. On the End of Privacy explores how literacy is transformed by online technology that lets us instantly publish anything that we can see or hear. Miller examines the 2010 suicide of Tyler Clementi, a young college student who jumped off the George Washington Bridge after he discovered that his roommate spied on him via webcam. With access to the text messages, tweets, and chatroom posts of those directly involved in this tragedy, Miller asks: why did no one intervene to stop the spying? Searching for an answer to that question leads Miller to online porn sites, the invention of Facebook, the court-martial of Chelsea Manning, the contents of Hillary Clinton's email server, Anthony Weiner's sexted images, Chatroulette, and more as he maps out the changing norms governing privacy in the digital age.

One woman's quest to discover the truth behind her husband's death will pit her against a new generation of cutting-edge surveillance technology and the most dangerous conspiracy in America—Invasion of Privacy is the riveting, new standalone suspense novel from New York Times bestselling author Christopher Reich. On a remote, dusty road forty miles outside of Austin, Texas, FBI agent Joe Grant and a confidential informant are killed in a deadly shootout. Left to pick up the pieces is Mary Grant, Joe's young wife and mother of their two daughters. The official report places blame for the deaths on Joe's shoulders . . . but the story just doesn't add up and Mary has too many troubling questions that need answers. How did Joe's final voice mail—containing a cryptic warning for Mary, recorded moments before the fatal shooting—disappear without a trace from her phone? Stonewalled by the FBI, Mary will be drawn into a deadly conspiracy that puts her in the crosshairs of the richest and most powerful men in America . . . and the newest and most terrifying surveillance system known to man. New York Times bestselling author Christopher Reich is the master of crafting thrillers of the highest caliber, with nonstop action and nail-biting suspense. Invasion of Privacy is his richest, most relevant novel to date and will have readers hooked from the first page to the last. Your privacy is for sale.

Organizations of all kinds are recognizing the crucial importance of protecting privacy. Their customers, employees, and other stakeholders demand it. Today, failures to safeguard privacy can destroy organizational reputations — and even the organizations themselves. But implementing effective privacy protection is difficult, and there are few comprehensive resources for those tasked with doing so. In Information Privacy Engineering and Privacy by Design, renowned information technology author William Stallings brings together the comprehensive and practical guidance you need to succeed. Stallings shows how to apply today's consensus best practices and widely-accepted standards documents in your environment, leveraging policy, procedures, and technology to meet legal and regulatory requirements and protect everyone who depends on you. Like Stallings' other award-winning texts, this guide is designed to help readers quickly find the information and gain the mastery needed to implement effective privacy. Coverage includes: Planning for privacy: Approaches for managing and controlling the privacy control function; how to define your IT environment's requirements; and how to develop appropriate policies and procedures for it Privacy threats: Understanding and identifying the full range of threats to privacy in information collection, storage, processing, access, and dissemination Information privacy technology: Satisfying the privacy requirements you've defined by using technical controls, privacy policies, employee awareness, acceptable use policies, and other techniques Legal and regulatory requirements: Understanding GDPR as well as the current spectrum of U.S. privacy regulations, with insight for mapping regulatory requirements to IT actions

Preserving Privacy in On-Line Analytical Processing (OLAP)

The Risks Posed by New Wiretapping Technologies

The End of Privacy

On the End of Privacy

Invasion of Privacy

Security and Privacy in Smart Sensor Networks