# Watching The Watchers Surveillance Transparency And

Digital communications technology has immeasurably enhanced our capacity to store, retrieve, and exchange information. But who controls our access to information, and who decides what others have a right to know about us? In Controlling Knowledge, author Lorna Stefanick offers a thoughtprovoking and eminently user-friendly overview of current legislation governing freedom of information and the protection of privacy. Aiming to clarify rather than mystify, Stefanick outlines the history and application of FOIP legislation, with special focus on how these laws affect the individual. To illustrate the impact of FOIP, she examines the notion of informed consent, looks at concerns about surveillance in the digital age, and explores the sometimes insidious influence of Facebook. Specialists in public policy and public administration, information technology, communications, law, criminal justice, sociology, and health care will find much here that bears directly on their work, while students and general readers will welcome the book's down-to-earth language and accessible style. Intended to serve as a "citizen's guide," Controlling Knowledge is a vital resource for anyone seeking to understand how freedom of information and privacy protection are legally defined

and how this legislation is shaping our individual rights as citizens of the information age. Lorna Stefanick is an associate professor in the Governance, Law, and Management program in the Centre for State and Legal Studies at Athabasca University.

Please Visit the Companion website:

www.aspenlawschool.com/dycus\_nationalsecurity4 For the broadest exploration of both constitutional and domestic law issues in national security, as well as thoughtful treatment of related international law topics

This multidisciplinary book introduces readers to original perspectives on crimmigration that foster holistic, contextual, and critical appreciation of the concept in Australia and its individual consequences and broader effects. This collection draws together contributions from nationally and internationally respected legal scholars and social scientists united by common and overlapping interests, who identify, critique, and reimagine crimmigration law and practice in Australia, and thereby advance understanding of this important field of inquiry. Specifically, crimmigration is addressed and analysed from a variety of standpoints, including: criminal law/justice; administrative law/justice; immigration law; international law; sociology of law; legal history feminist theory, settler colonialism, and political sociology. The book aims to: explore the Page 2/28

historical antecedents of contemporary crimmigration and continuities with the past in Australia reveal the forces driving crimmigration and explain its relationship to border securitisation in Australia identify and examine the different facets of crimmigration, comprising: the substantive overlaps between criminal and immigration law; crimmigration processes; investigative techniques, surveillance strategies, and law enforcement agents, institutions and practices uncover the impacts of crimmigration law and practice upon the human rights and interests of non-citizens and their families. analyse crimmigration from assorted critical standpoints; including settler colonialism, race and feminist perspectives By focusing upon these issues, the book provides an interconnected collection of chapters with a cohesive narrative, notwithstanding that contributors approach the themes and specific issues from different theoretical and critical standpoints, and employ a range of research methods.

Per millenni nel corso della storia umana dimenticare è stata la norma, e ricordare l'eccezione. Ma l'era digitale ha cambiato questo rapporto, creando un fenomeno completamente nuovo: oggi rimane traccia di tutto. Contenuti potenzialmente umilianti su Facebook restano conservati nel cyberspazio e potranno essere rivisti in futuro dagli utenti della Rete (inclusi il vostro partner o il datore di lavoro).

Google memorizza quando e che cosa abbiamo cercato. Lo spazio digitale ricorda anche quello che sarebbe meglio venisse dimenticato, e questo ha profonde implicazioni. Oggi il passato è sempre presente, pronto a essere richiamato con il semplice clic di un mouse. Si tratti di informazioni datate e astratte dal contesto originale o di foto compromettenti, il Web non ci permetterà di dimenticare. Il diritto alla privacy o altre normative analoghe non basteranno a proteggerci. Leggete il libro e capirete perché. E che cosa si può fare. Episodes in the history of data, from early modern math problems to today's inescapable "dataveillance," that demonstrate the dependence of data on culture. We live in the era of Big Data, with storage and transmission capacity measured not just in terabytes but in petabytes (where peta-denotes a quadrillion, or a thousand trillion). Data collection is constant and even insidious, with every click and every "like" stored somewhere for something. This book reminds us that data is anything but "raw," that we shouldn't think of data as a natural resource but as a cultural one that needs to be generated. protected, and interpreted. The book's essays describe eight episodes in the history of data from the predigital to the digital. Together they address such issues as the ways that different kinds of data and different domains of inquiry are mutually defining; how data are variously "cooked" in the Page 4/28

processes of their collection and use; and conflicts over what can--or can't--be "reduced" to data. Contributors discuss the intellectual history of data as a concept; describe early financial modeling and some unusual sources for astronomical data: discover the prehistory of the database in newspaper clippings and index cards; and consider contemporary "dataveillance" of our online habits as well as the complexity of scientific data curation. Essay Authors Geoffrey C. Bowker, Kevin R. Brine, Ellen Gruber Garvey, Lisa Gitelman, Steven J. Jackson, Virginia Jackson, Markus Krajewski, Mary Poovey, Rita Raley, David Ribes, Daniel Rosenberg, Matthew Stanley, Travis D. Williams Data access is essential for serving the public good. This book provides new frameworks to address the resultant privacy issues.

In a revealing study of how digital dossiers are created (usually without our knowledge), the author argues that we must rethink our understanding of what privacy is and what it means in the digital age, and then reform the laws that define and regulate it. Reprint.

Readers explore the worth of domestic surveillance and how it impacts the country. This volume also looks at the ethics of the National Security Agency as well as whether or not domestic surveillance needs more oversight. Fifteen different essays provide debate on both sides of every issues, allowing readers to sharpen

their critical thinking skills.

A free ebook version of this title is available through Luminos, University of California Press's new open access publishing program for monographs. Visit www.luminosoa.org to learn more. With Mexico's War on Crime as the backdrop, Making Things Stick offers an innovative analysis of how surveillance technologies impact governance in the global society. More than just tools to monitor ordinary people, surveillance technologies are imagined by government officials as a way to reform the national state by focusing on the material things—cellular phones, automobiles, human bodies—that can enable crime. In describing the challenges that the Mexican government has encountered in implementing this novel approach to social control, Keith Guzik presents surveillance technologies as a sign of state weakness rather than strength and as an opportunity for civic engagement rather than retreat.

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.

This book is nothing less than a complete and comprehensive survey of the state-of-the-art of terrorism informatics. It covers the application of advanced methodologies and information fusion and analysis. It also lays out techniques to acquire, integrate, process, analyze, and manage the diversity of terrorism-related information for international and homeland securityrelated applications. The book details three major areas of terrorism research: prevention, detection, and established governmental responses to terrorism. It systematically examines the current and ongoing research, including recent case studies and application of terrorism informatics techniques. The coverage then presents the critical and relevant social/technical areas to terrorism research including social, privacy, data confidentiality, and legal challenges.

This book tackles the regulatory issues of Unmanned Aerial Systems (UAS) or Remotely-Piloted Aerial Systems (RPAS), which have profound consequences for privacy, security and other fundamental liberties. Collectively known as "drones," they were initially

deployed for military purposes: reconnaissance, surveillance and extrajudicial executions. Today, we are witnessing a growth of their use into the civilian and humanitarian domain. They are increasingly used for goals as diverse as news gathering, aerial inspection of oil refinery flare stacks, mapping of the Amazonian rainforest, crop spraying and search and rescue operations. The civil use of drones is becoming a reality in the European Union and in the US. The drone revolution may be a new technological revolution. Proliferation of the next generation of "recreational" drones show how drones will be sold as any other consumer item. The cultural perception of the technology is shifting, as drones are increasingly being used for humanitarian activities, on one hand, but they can also firmly be situated in the prevailing modes of postmodern governance on the other hand. This work will be of interest to researchers in Criminology and Criminal Justice interested in issues related to surveillance. security, privacy, and technology. It will also provide a criminological background for related legal issues, such as privacy law, aviation law, international criminal law, and comparative law.

This Handbook presents innovative research that compares different criminal procedure systems by focusing on the mechanisms by which legal systems seek to avoid error, protect rights, ground their legitimacy, expand lay participation in the criminal process and develop alternatives to criminal trials, such as plea bargaining, as well as alternatives to the criminal process as a whole, such as intelligence operations. The

criminal procedures examined in this book include those of the United States, Germany, France, Spain, Russia, India, Latin America, Taiwan and Japan, among others. In New York and Baltimore, police cameras scan public areas twenty-four hours a day. Huge commercial databases track you finances and sell that information to anyone willing to pay. Host sites on the World Wide Web record every page you view, and "smart" toll roads know where you drive. Every day, new technology nibbles at our privacy. Does that make you nervous? David Brin is worried, but not just about privacy. He fears that society will overreact to these technologies by restricting the flow of information, frantically enforcing a reign of secrecy. Such measures, he warns, won't really preserve our privacy. Governments, the wealthy, criminals, and the techno-elite will still find ways to watch us. But we'll have fewer ways to watch them. We'll lose the key to a free society: accountability. The Transparent Society is a call for "reciprocal transparency." If police cameras watch us, shouldn't we be able to watch police stations? If credit bureaus sell our data, shouldn't we know who buys it? Rather than cling to an illusion of anonymity-a historical anomaly, given our origins in close-knit villageswe should focus on quarding the most important forms of privacy and preserving mutual accountability. The biggest threat to our freedom, Brin warns, is that surveillance technology will be used by too few people, now by too many. A society of glass houses may seem too fragile. Fearing technology-aided crime, governments seek to restrict online anonymity; fearing technologyaided tyranny, citizens call for encrypting all data. Brins

shows how, contrary to both approaches, windows offer us much better protection than walls; after all, the strongest deterrent against snooping has always been the fear of being spotted. Furthermore, Brin argues, Western culture now encourages eccentricity-we're programmed to rebel! That gives our society a natural protection against error and wrong-doing, like a body's immune system. But "social T-cells" need openness to spot trouble and get the word out. The Transparent Society is full of such provocative and far-reaching analysis. The inescapable rush of technology is forcing us to make new choices about how we want to live. This daring book reminds us that an open society is more robust and flexible than one where secrecy reigns. In an era of gnat-sized cameras, universal databases, and clothes-penetrating radar, it will be more vital than ever for us to be able to watch the watchers. With reciprocal transparency we can detect dangers early and expose wrong-doers. We can gauge the credibility of pundits and politicians. We can share technological advances and news. But all of these benefits depend on the free, twoway flow of information.

"They know where you got on the bus, where you went to work, where you slept, and what other cell phones slept with you." Edward Snowden The disclosures by Edward Snowden since June 2013 revealing mass surveillance and large-scale intrusion practices have provided compelling evidence of the existence of far-reaching, technologically advanced surveillance systems. Put in place by United States intelligence services and their partners in certain Council of Europe member states, these systems are aimed at collecting, storing and analysing communication data,

including content, location and other metadata, on a massive scale. In several countries, a massive "surveillance-industrial complex" has evolved, which risks escaping democratic control and accountability and threatens the free and open character of our societies. The surveillance practices disclosed endanger fundamental human rights, including the rights to privacy, freedom of information and expression, and the rights to a fair trial and freedom of religion. Given the threat such surveillance techniques pose, how can states uphold these fundamental rights and ensure the protection of privacy and Internet safety in the digital age? This book presents, in its first part, the report of the Parliamentary Assembly of the Council of Europe and, in its second part, the legal expertise of the European Commission for Democracy through Law (the Venice Commission).

Years of surveillance-related leaks from US whistleblower Edward Snowden have fuelled an international debate on privacy, spying, and Internet surveillance. Much of the focus has centered on the role of the US National Security Agency, yet there is an important Canadian side to the story. The Communications Security Establishment, the Canadian counterpart to the NSA, has played an active role in surveillance activities both at home and abroad, raising a host of challenging legal and policy questions. With contributions by leading experts in the field, Law, Privacy and Surveillance in Canada in the Post-Snowden Era is the right book at the right time: From the effectiveness of accountability and oversight programs to the legal issues raised by metadata collection to the privacy challenges surrounding new technologies, this book explores current issues torn from the headlines with a uniquely Canadian perspective. Transparency and Surveillance as Sociotechnical Accountability A House of Mirrors Routledge While traveling the data highway through the global village, Page 11/28

most people, if they think about it at all, consider privacy a non-forfeitable right. They expect to have control over the ways in which their personal information is obtained, distributed, shared, and used by any other entity. According to recent surveys, privacy, and anonymity are the fundamental issues of concern for most Internet users. ranked higher than ease-of-use, spam, cost, and security. Digital Privacy: Theory, Techniques, and Practices covers state-of-the-art technologies, best practices, and research results, as well as legal, regulatory, and ethical issues. Editors Alessandro Acquisti, Stefanos Gritzalis, Costas Lambrinoudakis, and Sabrina De Capitani di Vimercati, established researchers whose work enjoys worldwide recognition, draw on contributions from experts in academia, industry, and government to delineate theoretical, technical, and practical aspects of digital privacy. They provide an up-todate, integrated approach to privacy issues that spells out what digital privacy is and covers the threats, rights, and provisions of the legal framework in terms of technical counter measures for the protection of an individual's privacy. The work includes coverage of protocols, mechanisms, applications, architectures, systems, and experimental studies. Even though the utilization of personal information can improve customer services, increase revenues, and lower business costs, it can be easily misused and lead to violations of privacy. Important legal, regulatory, and ethical issues have emerged, prompting the need for an urgent and consistent response by electronic societies. Currently there is no book available that combines such a wide range of privacy topics with such a stellar cast of contributors. Filling that void, Digital Privacy: Theory, Techniques, and Practices gives you the foundation for building effective and legal privacy protocols into your business processes.

This book offers a new look at international security

management combining practical applications and theoretical foundations for new solutions to today's complex security and safety challenges. The book's focus on safety as a positive experience complements the traditional approach to safety as risks and threats. In addition, its multi-stakeholder, multi-disciplinary, international and evidence-based approach provides holistic and timely insights for the field. Topics raised in this book focus on the crucial questions of: Who is safety actually for? (and) How can sustainable safety solutions be jointly created? This book provides comprehensive insights into the latest research findings, practical applications and suggestions for dealing with challenges in international security management in integrated and sustainable ways. making it relevant reading for practitioners, as well as academics and students - with a view to obtaining thorough, first-hand knowledge from serving experts in the field. We explore new ways of working with citizens, police and policymakers in order to co-create safety. This book emphasises the importance of safety as a topic that matters for all. "Safety and security are basic pillars for the development of our society. However, the number of areas, actors and procedures involved in the management of the different elements composing the international security ecosystem, its coordination and alignment, make it a challenging issue to resolve. This book provides a fresh new approach to this complex issue, in which we all have a role to play." Fernando Ruiz, Acting Head of European Cyber-Crime Centre - Europol "A very timely analysis that brings a muchneeded international perspective to the field of security management. The authors explore the challenges confronting security management in a complex and connected world and generate new ideas to support practice and inspire research." Professor Mark Griffin; John Curtin Distinguished Professor, Curtin University; Director, Future of Work Institute "This

book presents the role of International Security Management in the 21st century in an innovative way." Dr. Christian Endreß, Managing Director, ASW Bundesverband - German Association for Security in Industry and Commerce What limits, if any, should be placed on a government's efforts to spy on its citizens in the interests of national security? Spying on foreigners has long been regarded as an unseemly but necessary enterprise. Spying on one's own citizens in a democracy, by contrast, has historically been subject to various forms of legal and political restraint. For most of the twentieth century these regimes were kept distinct. That position is no longer tenable. Modern threats do not respect national borders. Changes in technology make it impractical to distinguish between 'foreign' and 'local' communications. And our culture is progressively reducing the sphere of activity that citizens can reasonably expect to be kept from government eyes. The main casualty of this transformed environment will be privacy. Recent battles over privacy have been dominated by fights over warrantless electronic surveillance or CCTV; the coming years will see debates over data-mining and biometric identification. There will be protests and lawsuits, editorials and elections resisting these attacks on privacy. Those battles are worthy. But they will all be lost. Modern threats increasingly require that governments collect such information, governments are increasingly able to collect it, and citizens increasingly accept that they will collect it. The point of this book is to shift focus away from questions of whether governments should collect information and onto more problematic and relevant questions concerning its use. By reframing the relationship between privacy and security in the language of a social contract, mediated by a citizenry who are active participants rather than passive targets, the book offers a framework to defend freedom without sacrificing liberty.

"An admirably clear-sighted and engaging analysis of contemporary forms of mediation, illuminating the dynamics of new media across social, political and cultural spheres... Eugenia Siapera provokes her reader to think afresh about familiar phenomena, to synthesise diverse theoretical positions, and to stretch their imaginations to anticipate what is coming." - Sonia Livingstone, London School of Economics and Political Science "An excellent introduction to the past, present and future of the electronic, networked media world. By carefully examining the complex interactions between society and media, Siapera insightfully illuminates the social, political, economic and cultural consequences of our increasingly electronically networked and mediated world... a highly useful teaching tool and an engaging read for students, teachers and scholars." - Steve Jones, University of Illinois, Chicago New media are everywhere, yet with so many technological developments and theoretical perspectives understanding them has never been more difficult. Eugenia Siapera explains the key concepts and approaches to the impact of new media on the economy, society, identity, politics, friendship, citizenship and everyday life. Putting the student first, this book: Engages the reader with integrated, up-to-date case studies Brings it all together with chapter summary charts Challenges students to apply concepts with etivities Provides key further online readings here This book is both starting point and map for any student of new media and digital culture.

No country, no culture, no person today is untouched by what happens in the rest of the world. Technological innovation, environmental degradation, economic gain & loss, nuclear weapons, instant communication have all created unprecedented familiarity among the world's many cultures. With this historic development, the Dalai

Lama understands that the essential task of humanity in the 21st Century is to cultivate peaceful coexistence. Many believe in the inevitability of an escalating "clash of civilizations". Peaceful coexistence has long been problematic with religion, and while previous conflicts over religious differences may have been significant and regrettable, they did not threaten the very survival of humanity. Now, when extremists can persuade followers with the immense emotional power of faith and have access to powerful technological resources, a single spark could ignite a powder keg of frightening proportions. Yet the Dalai Lama shows how the challenges of globalization can also move us in another direction, to a deeper plane where nations, cultures, and individuals connect through their shared human nature. All major religions confront the same perennial questions; each have distinct forms of expression. But this marvelous diversity of insight has the potential for inspiring dialogue which can enrich everyone's pursuit of wisdom. All faith traditions turn to compassion as a guiding principle for living a good life. It is the task of all people with an aspiration to spiritual perfection to affirm the fundamental value of the compassion. In this way we can truly develop a deep recognition of the value of other faiths, and on that basis, we can cultivate genuine respect. In Toward a True Kinship of Faiths, the Dalai Lama also explores where differences between religions can be genuinely appreciated without serving as a source of conflict. The establishment of genuine harmony is not dependent upon accepting that all religions are fundamentally the same or that they lead to

the same place. Many fear that recognizing the value of another faith is incompatible with having devotion to the truth of one's own. Nevertheless, the Dalai Lama profoundly shows how a sincere believer can, with integrity, be a pluralist in relation to other religions without compromising commitment to the essence of the doctrinal teachings of their own faith. An issue of central importance for the Dalai Lama personally and for the entire world in general, Toward a True Kinship of Faiths offers a hopeful yet realistic look at how humanity must step into the future.

Can we safeguard our nation's security without weakening cherished liberties? And how does technology affect the potential conflict between these fundamental goals? These questions acquired renewed urgency in the wake of the 9/11 attacks. They also spurred heated debates over such controversial measures as Total Information Awareness and the USA PATRIOT Act. In this volume, leading figures from the worlds of government, public policy, and business analyze the critical issues underlying these debates. The first set of essays examines the relationship between liberty and security and explores where the public stands on how best to balance the two. In the second section, the authors focus on information technology's role in combating terrorism, as well as tools, policies, and procedures that can strengthen both security and liberty at the same time. Finally, the third part of the book takes on a series of key legal issues concerning the restrictions that should be placed on the government's power to exploit these powerful new technologies. Contributors

include Zoë Baird (Markle Foundation), James Barksdale (Barksdale Group), Bruce Berkowitz (Hoover Institution), Jerry Berman (Center for Democracy and Technology), Beryl A. Howell (Stroz Friedberg), Jon Kyl (U.S. Senate), Gilman Louie (In-Q-Tel), David Luban (Georgetown University), Richard A. Posner (U.S. Court of Appeals for the Seventh Circuit), Marc Rotenberg (Electronic Privacy Information Center), James Steinberg (Brookings), Larry Thompson (Brookings), Gayle von Eckartsberg (In-Q-Tel), and Alan F. Westin (Columbia University). This groundbreaking book introduces the application of statistical methodologies to e-Commerce data With the expanding presence of technology in today's economic market, the use of the Internet for buying, selling, and investing is growing more popular and public in nature. Statistical Methods in e-Commerce Research is the first book of its kind to focus on the statistical models and methods that are essential in order to analyze information from electronic-commerce (e-Commerce) transactions, identify the challenges that arise with new e-Commerce data structures, and discover new knowledge about consumer activity. This collection gathers over thirty researchers and practitioners from the fields of statistics, computer science, information systems, and marketing to discuss the growing use of statistical methods in e-Commerce research. From privacy protection to economic impact, the book first identifies the many obstacles that are encountered while collecting, cleaning, exploring, and analyzing e-Commerce data. Solutions to these problems are then suggested using established and newly developed

statistical and data mining methods. Finally, a look into the future of this evolving area of study is provided through an in-depth discussion of the emerging methods for conducting e-Commerce research. Statistical Methods in e-Commerce Research successfully bridges the gap between statistics and e-Commerce, introducing a statistical approach to solving challenges that arise in the context of online transactions, while also introducing a wide range of e-Commerce applications and problems where novel statistical methodology is warranted. It is an ideal text for courses on e-Commerce at the upperundergraduate and graduate levels and also serves as a valuable reference for researchers and analysts across a wide array of subject areas, including economics, marketing, and information systems who would like to gain a deeper understanding of the use of statistics in their work.

Surveillance in Europe is an accessible, definitive and comprehensive overview of the rapidly growing multi-disciplinary field of surveillance studies in Europe.

Written by experts in the field, including leading scholars, the Companion's clear and up to date style will appeal to a wide range of scholars and students in the social sciences, arts and humanities. This book makes the case for greater resilience in European society in the face of the growing pervasiveness of surveillance. It examines surveillance in Europe from several different perspectives, including: the co-evolution of surveillance technologies and practices the surveillance industry in Europe the instrumentality of surveillance for preventing and detecting crime and terrorism social and economic

costs impacts of surveillance on civil liberties resilience in Europe's surveillance society, the consequences and impacts for Europe of the Snowden revelations findings and recommendations regarding surveillance in Europe Surveillance in Europe's interdisciplinary approach and accessible content makes it an ideal companion to academics, policy-makers and civil society organisations alike, as well as appealing to top level undergraduates and postgraduates.

The 21st century offers a dizzying array of new technological developments: robots smart enough to take white collar jobs, social media tools that manage our most important relationships, ordinary objects that track, record, analyze and share every detail of our daily lives, and biomedical techniques with the potential to transform and enhance human minds and bodies to an unprecedented degree. Emerging technologies are reshaping our habits, practices, institutions, cultures and environments in increasingly rapid, complex and unpredictable ways that create profound risks and opportunities for human flourishing on a global scale. How can our future be protected in such challenging and uncertain conditions? How can we possibly improve the chances that the human family will not only live, but live well, into the 21st century and beyond? This book locates a key to that future in the distant past: specifically, in the philosophical traditions of virtue ethics developed by classical thinkers from Aristotle and Confucius to the Buddha. Each developed a way of seeking the good life that equips human beings with the moral and intellectual character to flourish even in the

most unpredictable, complex and unstable situations--precisely where we find ourselves today. Through an examination of the many risks and opportunities presented by rapidly changing technosocial conditions, Vallor makes the case that if we are to have any real hope of securing a future worth wanting, then we will need more than just better technologies. We will also need better humans. Technology and the Virtues develops a practical framework for seeking that goal by means of the deliberate cultivation of technomoral virtues specific skills and strengths of character, adapted to the unique challenges of 21st century life, that offer the human family our best chance of learning to live wisely and well with emerging technologies.

Focusing on the role of the state in defending against cyber threats and in securing the information age, this volume intrigues and provokes with a number of 'fresh' hypotheses, observations and suggestions. It contributes to mapping the diverse layers, actors, approaches and policies of the cyber security realm.

How do you find your way in an age of information overload? How can you filter streams of complex information to pull out only what you want? Why does it matter how information is structured when Google seems to magically bring up the right answer to your questions? What does it mean to be "findable" in this day and age? This eye-opening new book examines the convergence of information and connectivity. Written by Peter Morville, author of the groundbreaking Information Architecture for the World Wide Web, the book defines our current age as a state of unlimited findability. In other words, anyone

can find anything at any time. Complete navigability. Morville discusses the Internet, GIS, and other network technologies that are coming together to make unlimited findability possible. He explores how the melding of these innovations impacts society, since Web access is now a standard requirement for successful people and businesses. But before he does that, Morville looks back at the history of wayfinding and human evolution, suggesting that our fear of being lost has driven us to create maps, charts, and now, the mobile Internet. The book's central thesis is that information literacy. information architecture, and usability are all critical components of this new world order. Hand in hand with that is the contention that only by planning and designing the best possible software, devices, and Internet, will we be able to maintain this connectivity in the future. Morville's book is highlighted with full color illustrations and rich examples that bring his prose to life. Ambient Findability doesn't preach or pretend to know all the answers. Instead, it presents research, stories, and examples in support of its novel ideas. Are we truly at a critical point in our evolution where the quality of our digital networks will dictate how we behave as a species? Is findability indeed the primary key to a successful global marketplace in the 21st century and beyond. Peter Morville takes you on a thought-provoking tour of these memes and more -- ideas that will not only fascinate but will stir your creativity in practical ways that you can apply to your work immediately. "A lively, enjoyable and informative tour of a topic that's only going to become more important." -- David Weinberger, Author,

Small Pieces Loosely Joined and The Cluetrain Manifesto "I envy the young scholar who finds this inventive book, by whatever strange means are necessary. The future isn't just unwritten--it's unsearched." -- Bruce Sterling, Writer, Futurist, and Co-Founder. The Electronic Frontier Foundation "Search engine marketing is the hottest thing in Internet business, and deservedly so. Ambient Findability puts SEM into a broader context and provides deeper insights into human behavior. This book will help you grow your online business in a world where being found is not at all certain." -- Jakob Nielsen, Ph.D., Author, Designing Web Usability: The Practice of Simplicity "Information that's hard to find will remain information that's hardly found--from one of the fathers of the discipline of information architecture, and one of its most experienced practitioners, come penetrating observations on why findability is elusive and how the act of seeking changes us." -- Steve Papa, Founder and Chairman, Endeca "Whether it's a fact or a figure, a person or a place, Peter Morville knows how to make it findable. Morville explores the possibilities of a world where everything can always be found--and the challenges in getting there--in this wide-ranging, thought-provoking book." -- Jesse James Garrett, Author, The Elements of User Experience "It is easy to assume that current searching of the World Wide Web is the last word in finding and using information. Peter Morville shows us that search engines are just the beginning. Skillfully weaving together information science research with his own extensive experience, he develops for the reader a feeling for the near future when

information is truly findable all around us. There are immense implications, and Morville's lively and humorous writing brings them home." -- Marcia J. Bates, Ph.D., University of California Los Angeles "I've always known that Peter Morville was smart. After reading Ambient Findability, I now know he's (as we say in Boston) wicked smart. This is a timely book that will have lasting effects on how we create our future. -- Jared Spool, Founding Principal, User Interface Engineering "In Ambient Findability, Peter Morville has put his mind and keyboard on the pulse of the electronic noosphere. With tangible examples and lively writing, he lays out the challenges and wonders of finding our way in cyberspace, and explains the mutually dependent evolution of our changing world and selves. This is a must read for everyone and a practical guide for designers." -- Gary Marchionini, Ph.D., University of North Carolina "Find this book! Anyone interested in making information easier to find, or understanding how finding and being found is changing, will find this thoroughly researched, engagingly written, literate, insightful and very, very cool book well worth their time. Myriad examples from rich and varied domains and a valuable idea on nearly every page. Fun to read, too! --Joseph Janes, Ph.D., Founder, Internet Public Library The ability to forget, or be forgotten, has played an important part in human society, allowing for changed minds, second chances and overlooked embarrassments. Digital technology, with its inexhaustible memory, threatens one of the most important social conventions: the past is past. This book

explores the issues.

Draws together contributions from leading figures in the field of surveillance to engage in the discussion of the emergence of accountability as a means to manage threats to privacy. The first of its kind to enrich the debate about accountability and privacy by drawing together perspectives from experienced privacy researchers and policy makers.

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 explains the different approaches to interpreting the Fourth Amendment that the Supreme Court has used throughout American history, concentrating on the changes in interpretation since the Court applied the exclusionary rule to the states in 1961. It examines the evolution of the warrant rule and the exceptions to it, the reasonableness approach, the special needs approach, individual and society expectations of privacy, and the role of the exclusionary rule.

Describes the social and human cost of the security measures taken by the United States during the past decade.

Surveillance and transparency are both significant and increasingly pervasive activities in neoliberal societies. Surveillance is taken up as a means to achieving security and efficiency; transparency is seen as a

mechanism for ensuring compliance or promoting informed consumerism and informed citizenship. Indeed, transparency is often seen as the antidote to the threats and fears of surveillance. This book adopts a novel approach in examining surveillance practices and transparency practices together as parallel systems of accountability. It presents the house of mirrors as a new framework for understanding surveillance and transparency practices instrumented with information technology. The volume centers around five case studies: Campaign Finance Disclosure, Secure Flight, American Red Cross, Google, and Facebook. A series of themed chapters draw on the material and provide crosscase analysis. The volume ends with a chapter on policy implications.

The terrorist attacks of September 11, 2001, and the ensuing 'war on terror' have focused attention on issues that have previously lurked in a dark corner at the edge of the legal universe. This book presents a systematic and comprehensive attempt by legal scholars to conceptualize the theory of emergency powers, combining post-September 11 developments with more general theoretical, historical and comparative perspectives. The authors examine the interface between law and violent crises through history and across jurisdictions, bringing together insights gleaned from the Roman republic and Jewish law through to the initial responses to the July 2005 attacks in London. Three models of emergency powers are used to offer a conceptualization of emergency regimes, giving a coherent insight into law's interface with and regulation

of crisis and a distinctive means to evaluate the legal options open to states for dealing with crises.

Copyright: 4a0d0d6d990abb4293dad920d4905801