Data And Goliath The Hidden Battles To Collect Your Data And Control Your World

Yeah, reviewing a ebook **Data And Goliath The Hidden Battles To Collect Your Data And Control Your World** could accumulate your close links listings. This is just one of the solutions for you to be successful. As understood, success does not suggest that you have extraordinary points.

Comprehending as without difficulty as settlement even more than new will have enough money each success. adjacent to, the revelation as without difficulty as keenness of this Data And Goliath The Hidden Battles To Collect Your Data And Control Your World can be taken as competently as picked to act.

The Future of Violence - Robots and Germs, Hackers and Drones Benjamin Wittes 2016-03-15 The terrifying new role of technology in a world at war

The Beautiful Struggle (Adapted for Young Adults) Ta-Nehisi Coates 2022-01-11 "A memoir from Ta-Nehisi Coates, in which he details the challenges on the streets and within one's family, especially the eternal struggle for peace between a father and son and the important role family plays in such circumstances"--

Listening in Susan Eva Landau 2017-01-01 A cybersecurity expert and former Google privacy analyst's urgent call to protect devices and networks against malicious hackers New technologies have provided both incredible convenience and new threats. The same kinds of digital networks that allow you to hail a ride using your smartphone let power grid operators control a country's electricity--and these personal, corporate, and government systems are all vulnerable. In Ukraine, unknown hackers shut off electricity to nearly 230,000 people for six hours. North Korean hackers destroyed networks at Sony Pictures in retaliation for a film that mocked Kim Jong-un. And Russian cyberattackers leaked Democratic National Committee emails in an attempt to sway a U.S. presidential election. And yet despite such documented risks, government agencies, whose investigations and surveillance are stymied by encryption, push for a weakening of protections. In this accessible and riveting read, Susan Landau makes a compelling case for the need to secure our data, explaining how we must maintain cybersecurity in an insecure age.

Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World Bruce Schneier 2015-03-02 “Bruce Schneier’s amazing book is the best overview of privacy and security ever written.”—Clay Shirky “Bruce Schneier’s amazing book is the best overview of privacy and security ever written.”—Clay Shirky Your cell phone provider tracks your location and knows who’s with you. Your online and in-store purchasing patterns are recorded, and reveal if you're unemployed, sick, or pregnant. Your e-mails and texts expose your intimate and casual friends. Google knows what you’re thinking because it saves your private searches. Facebook can determine your sexual orientation without you ever mentioning it. The powers that surveil us do more than simply store this information. Corporations use surveillance to manipulate not only the news articles and advertisements we each see, but also the prices we’re offered. Governments use surveillance to discriminate, censor, chill free speech, and put people in danger worldwide. And both sides share this information with each other or, even worse, lose it to cybercriminals in huge data breaches. Much of this is voluntary: we cooperate with corporate surveillance because it promises us convenience, and we submit to government surveillance because it promises us protection. The result is a mass surveillance society of our own making. But have we given up more than we’ve gained? In Data and Goliath, security expert Bruce Schneier offers another path, one that values both security and privacy. He brings his bestseller up-to-date with a new preface covering the latest developments, and then shows us exactly what we can do to reform government surveillance programs, shake up surveillance-based business models, and protect our individual privacy. You'll never look at your phone, your computer, your credit cards, or even your car in the same way again.

Carry On Bruce Schneier 2013-12-16 A look at the world of twenty-first-century security features over 150 of the author's commentaries on such topics as airport surveillance, cyberterrorism, privacy, and the economics of security.

The Code Margaret O'Mara 2020-07-07 One of New York Magazine's best books on Silicon Valley! The true, behind-the-scenes history of the people who built Silicon Valley and shaped Big Tech in America Long before Margaret O'Mara became one of our most consequential historians of the American-led digital revolution, she worked in the White House of Bill Clinton and Al Gore in the earliest days of the commercial Internet. There she saw firsthand how deeply intertwined Silicon Valley was with the federal government--and always had been--and how shallow the common understanding of the secrets of the Valley's success actually was. Now, after almost five years of pioneering research, O'Mara has produced the definitive history of Silicon Valley for our time, the story of mavericks and visionaries, but also of powerful institutions creating the framework for innovation, from the Pentagon to Stanford University. It is also a story of a community that started off remarkably homogeneous and tight-knit and stayed that way, and whose belief in its own mythology has deepened into a collective hubris that has led to astonishing triumphs as well as devastating second-order effects. Deploying a wonderfully rich and diverse cast of protagonists, from the justly famous to the unjustly obscure, across four generations of explosive growth in the Valley, from the forties to the present, O'Mara has wrestled one of the most fateful developments in modern American history into magnificent narrative form. She is on the ground with all of the key tech companies, chronicling the evolution in their offerings through each successive era, and she has a profound fingertip feel for the politics of the sector and its relation to the larger cultural narrative about tech as it has evolved over the years. Perhaps most impressive, O'Mara has penetrated the inner kingdom of tech venture capital firms, the insular and still remarkably old-boy world that became the cockpit of American capitalism and the crucible for bringing technological innovation to market, or not. The transformation of big tech into the engine room of the American economy and the nexus of so many of our hopes and dreams--and, increasingly, our nightmares--can be understood, in Margaret O'Mara's masterful hands, as the story of one California valley. As her majestic history makes clear, its fate is the fate of us all.

Economics of Information Security and Privacy III Bruce Schneier 2012-09-26 The Workshop on the Economics of Information Security (WEIS) is the leading forum for interdisciplinary scholarship on information security, combining expertise from the fields of economics, social science, business, law, policy and computer science. Prior workshops have explored the role of incentives between attackers and defenders, identified market failures dogging Internet security, and assessed investments in cyber-defense. Current contributions build on past efforts using empirical and analytic tools to not only understand threats, but also strengthen security through novel evaluations of available solutions. Economics of Information Security and Privacy III addresses the following questions: how should information risk be modeled given the constraints of rare incidence and high interdependence; how do individuals' and organizations' perceptions of privacy and security color their decision making; how can we move towards a more secure information infrastructure and code base while accounting for the incentives of stakeholders?

Schneier on Security Bruce Schneier 2009-03-16 Presenting invaluable advice from the world?s most famous computer security expert, this intensely readable collection features some of the most insightful and informative coverage of the strengths and weaknesses of computer security and the price people pay -- figuratively and literally -- when security fails. Discussing the issues surrounding things such as airplanes, passports, voting machines, ID cards, cameras, passwords, Internet banking, sporting events, computers, and castles, this book is a must-read for anyone who values security at any level -- business, technical, or personal.

Army of None: Autonomous Weapons and the Future of War Paul Scharre 2018-04-24 "The book I had been waiting for. I can't recommend it highly enough." —Bill Gates The era of autonomous weapons has arrived. Today around the globe, at least thirty nations have weapons that can search for and destroy enemy targets all on their own. Paul Scharre, a leading expert in next-generation warfare, describes these and other high tech weapons systems—from Israel’s Harpy drone to the American submarine-hunting robot ship Sea Hunter—and examines the legal and ethical issues surrounding their use. “A smart primer to what’s to come in warfare” (Bruce Schneier), Army of None engages military history, global policy, and cutting-edge science to explore the implications of giving weapons the freedom to make life and death decisions. A former soldier himself, Scharre argues that we must embrace technology where it can make war more precise and humane, but when the choice is life or death, there is no replacement for the human heart.

Applied Cryptography Bruce Schneier 2015 From the world's most renowned security technologist, Bruce Schneier, this 20th Anniversary Edition is the most definitive reference on cryptography ever published and is the seminal work on cryptography. Cryptographic techniques have applications far beyond the obvious uses of encoding and decoding information. For developers who need to know about capabilities, such as digital signatures, that depend on cryptographic techniques, there's no better overview than Applied Cryptography, the definitive book on the subject. Bruce Schneier covers general classes of cryptographic protocols and then specific techniques, detailing the inner workings of real-world cryptographic algorithms including the Data Encryption Standard and RSA public-key cryptosystems. The book includes source-code listings and extensive advice on the practical aspects of cryptography implementation, such as the importance of generating truly random numbers and of keeping keys secure. ". . .the best introduction to cryptography I've ever seen. . . .The book the National Security Agency wanted never to be published. . . ." -Wired Magazine ". . .monumental . . . fascinating . . . comprehensive . . . the definitive work on cryptography for computer programmers . . ." -Dr. Dobb's Journal ". . .easily ranks as one of the most authoritative in its field." -PC Magazine The book details how programmers and electronic communications professionals can use cryptography-the technique of enciphering and deciphering messages-to maintain the privacy of computer data. It describes dozens of cryptography algorithms, gives practical advice on how to implement them into cryptographic software, and shows how they can be used to solve security problems. The book shows programmers who design computer applications, networks, and storage systems how they can build security into their software and systems. With a new Introduction by the author, this premium edition will be a keepsake for all those committed to computer and cyber security.

Aspen Treatise for National Security Law Geoffrey S. Corn 2019-05-24 This unique new concise treatise provides a highly accessible but also comprehensive and timely supplement for students studying National Security Law. Written by a team of experts in the field, this treatise serves as a useful supplement for the substantively rich but often overwhelming National Security Law texts currently on the market. Key Features Comprehensive overview of both the general legal framework for national security decision-making and commonly explored specific national security topics. Narrative explanation of complex jurisprudential, statutory, treaty, and regulatory sources of national security law. Complements a range of the most commonly addressed national security topics.

The Hacker and the State Ben Buchanan 2020-02-28 “One of the finest books on information security published so far in this century—easily accessible, tightly argued, superbly well-sourced, intimidatingly perceptive.” —Thomas Rid, author of Active Measures “The best examination I have read of how increasingly dramatic developments in cyberspace are defining the ‘new normal’ of geopolitics in the digital age. Buchanan...captures the dynamics of all of this truly brilliantly.” —General David Petraeus, former Director of the CIA and Commander of Coalition Forces in Iraq and Afghanistan Few national-security threats are as potent—or as nebulous—as cyber attacks. Ben Buchanan reveals how hackers are transforming spycraft and statecraft, catching us all in the crossfire, whether we know it or not. Ever since WarGames, we have been bracing for the cyberwar to come, conjuring images of exploding power plants and mass panic. But while cyber attacks are now disturbingly common, they don’t look anything like we thought they would. Packed with insider information based on interviews, declassified files, and forensic analysis of company reports, The Hacker and the State sets aside fantasies of cyber-annihilation to explore the real geopolitical competition of the digital age. Tracing the conflict of wills and interests among modern nations, Ben Buchanan reveals little-known details of how China, Russia, North Korea, Britain, and the United States hack one another in a relentless struggle for dominance. His analysis moves deftly from underseas cable taps to underground nuclear sabotage, from blackouts and data breaches to billion-dollar heists and election interference. Buchanan brings to life this continuous cycle of espionage and deception, attack and counterattack, destabilization and retaliation. He explains why cyber attacks are far less destructive than we anticipated, far more pervasive, and much harder to prevent. With little fanfare and far less scrutiny, they impact our banks, our tech and health systems, our democracy, and every aspect of our lives. Quietly, insidiously, they have reshaped our national-security priorities and transformed spycraft and statecraft. The contest for geopolitical advantage has moved into cyberspace. The United States and its allies can no longer dominate the way they once did. The nation that hacks best will triumph.

Data and Goliath Bruce Schneier 2016-02-08 Your cell phone provider knows your location; vendors record your purchasing patterns; your e-mails, texts, and social network activity are stored indefinitely; and all of this information is used by corporations and governments to manipulate, discriminate, and censor your experiences. The result is a mass surveillance society of our own making. Security expert Bruce Schneier offers another path, showing us exactly what we can do to reform government surveillance programs, shake up surveillance-based business models, and protect our individual privacy. From back cover.

Liars and Outliers Bruce Schneier 2012-01-27 In today's hyper-connected society, understanding the mechanisms of trust is crucial. Issues of trust are critical to solving problems as diverse as corporate responsibility, global warming, and the political system. In this insightful and entertaining book, Schneier weaves together ideas from across the social and biological sciences to explain how society induces trust. He shows the unique role of trust in facilitating and stabilizing human society. He discusses why and how trust has evolved, why it works the way it does, and the ways the information society is changing everything.

Tools and Weapons Brad Smith 2019-09-10 The New York Times bestseller, now updated with new material on cyber attacks, digital sovereignty, and tech in a pandemic. From Microsoft's president and one of the tech industry's broadest thinkers, a frank and thoughtful reckoning with how to balance enormous promise and existential risk as the digitization of everything accelerates. “A colorful and insightful insiders’ view of how technology is both empowering and threatening us. From privacy to cyberattacks, this timely book is a useful guide for how to navigate the digital future.” —Walter Isaacson Microsoft president Brad Smith operates by a simple core belief: When your technology changes the world, you bear a responsibility to help address the world you have helped create. In Tools and Weapons, Brad Smith and Carol Ann Browne bring us a captivating narrative from the top of Microsoft, as the company flies in the face of a tech sector long obsessed with disruption as an end in itself, and in doing so navigates some of the thorniest issues of our time—from privacy to cyberwar to the challenges

for democracy, far and near. As the tumultuous events of 2020 brought technology and Big Tech even further into the lives of almost all Americans, Smith and Browne updated the book throughout to reflect a changed world. With three new chapters on cybersecurity, technology and nation-states, and tech in the pandemic, Tools and Weapons is an invaluable resource from the cockpit of one of the world's largest tech companies.

Internet Privacy Rights Paul Bernal 2014-03-27 What rights to privacy do we have on the internet, and how can we make them real?

A New History of Modern Computing Thomas Haigh 2021-09-14 How the computer became universal. Over the past fifty years, the computer has been transformed from a hulking scientific supertool and data processing workhorse, remote from the experiences of ordinary people, to a diverse family of devices that billions rely on to play games, shop, stream music and movies, communicate, and count their steps. In A New History of Modern Computing, Thomas Haigh and Paul Ceruzzi trace these changes. A comprehensive reimagining of Ceruzzi's A History of Modern Computing, this new volume uses each chapter to recount one such transformation, describing how a particular community of users and producers remade the computer into something new. Haigh and Ceruzzi ground their accounts of these computing revolutions in the longer and deeper history of computing technology. They begin with the story of the 1945 ENIAC computer, which introduced the vocabulary of "programs" and "programming," and proceed through email, pocket calculators, personal computers, the World Wide Web, videogames, smart phones, and our current world of computers everywhere--in phones, cars, appliances, watches, and more. Finally, they consider the Tesla Model S as an object that simultaneously embodies many strands of computing.

We Have Root Bruce Schneier 2019-08-08 A collection of popular essays from security guru Bruce Schneier In his latest collection of essays, security expert Bruce Schneier tackles a range of cybersecurity, privacy, and real-world security issues ripped from the headlines. Essays cover the ever-expanding role of technology in national security, war, transportation, the Internet of Things, elections, and more. Throughout, he challenges the status quo with a call for leaders, voters, and consumers to make better security and privacy decisions and investments. Bruce's writing has previously appeared in some of the world's best-known and most-respected publications, including The Atlantic, the Wall Street Journal, CNN, the New York Times, the Washington Post, Wired, and many others. And now you can enjoy his essays in one place—at your own speed and convenience. • Timely security and privacy topics • The impact of security and privacy on our world • Perfect for fans of Bruce's blog and newsletter • Lower price than his previous essay collections The essays are written for anyone who cares about the future and implications of security and privacy for society.

Cult of the Dead Cow Joseph Menn 2019-06-04 The shocking untold story of the elite secret society of hackers fighting to protect our privacy, our freedom -- even democracy itself Cult of the Dead Cow is the tale of the oldest, most respected, and most famous American hacking group of all time. Though until now it has remained mostly anonymous, its members invented the concept of hacktivism, released the top tool for testing password security, and created what was for years the best technique for controlling computers from afar, forcing giant companies to work harder to protect customers. They contributed to the development of Tor, the most important privacy tool on the net, and helped build cyberweapons that advanced US security without injuring anyone. With its origins in the earliest days of the Internet, the cDc is full of oddball characters -- activists, artists, even future politicians. Many of these hackers have become top executives and advisors walking the corridors of power in Washington and Silicon Valley. The most famous is former Texas Congressman and current presidential candidate Beto O'Rourke, whose time in the cDc set him up to found a tech business, launch an alternative publication in El Paso, and make long-shot bets on unconventional campaigns. Today, the group and its followers are battling electoral misinformation, making personal data safer, and battling to keep technology a force for good instead of for surveillance and oppression. Cult of the Dead Cow shows how governments, corporations, and criminals came to hold immense power over individuals and how we can fight back against them.

Privacy in the Age of Big Data Theresa Payton 2014-01-16 Digital data collection and surveillance is pervasive and no one can protect your privacy without your help. Before you can help yourself, you need to understand the new technologies, what benefits they provide, and what trade-offs they require. Some of those trade-offs – privacy for convenience – could be softened by our own behavior or be reduced by legislation if we fight for it. This book analyzes why privacy is important to all of us, and it describes the technologies that place your privacy most at risk, starting with modern computing and the Internet.

Property Rights in Personal Data Nadezhda Purtova 2012 Personal data, at least in the European legal lexicon, is not a conventional object of property rights. Yet, regardless of the actual legal circumstances, lively markets in personal data have become a reality. The so-called information industry routinely collects and deals in databases containing personal details of people as both citizens and consumers, and appears to regard this data as its property. Moreover, individuals also treat data pertaining to them as their own, and habitually disclose personal data in exchange for money, goods, services, and online social interaction. This important new book defends the ground-breaking proposal to propertise personal data. Propertisation arguably improves the position of a data subject to exercise control over his/her personal data by creating more effective tools of accountability and monitoring. It can also be used, the author shows, to enforce existing data protection rights as expressed in the EC Data Protection Directive (1995), Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms (1945) and Convention No. 108 (1981). This book inquires to what extent the propertisation of personal data is legally possible in Europe, and examines what benefits and limitations would ensue. It provides: a systematic understanding of the developments and concerns with regard to personal data; a detailed examination of the main arguments for and against the concept of property in personal data; and a European perspective on property rights in personal data. The result is a book full of original insights that breaks new ground in addressing the problems of personal data in the European law of data protection and informational privacy."

Cryptography Engineering Niels Ferguson 2011-02-02 The ultimate guide to cryptography, updated from an author team of the world's top cryptography experts. Cryptography is vital to keeping information safe, in an era when the formula to do so becomes more and more challenging. Written by a team of world-renowned cryptography experts, this essential guide is the definitive introduction to all major areas of cryptography: message security, key negotiation, and key management. You'll learn how to think like a cryptographer. You'll discover techniques for building cryptography into products from the start and you'll examine the many technical changes in the field. After a basic overview of cryptography and what it means today, this indispensable resource covers such topics as block ciphers, block modes, hash functions, encryption modes, message authentication codes, implementation issues, negotiation protocols, and more. Helpful examples and hands-on exercises enhance your understanding of the multi-faceted field of cryptography. An author team of internationally recognized cryptography experts updates you on vital topics in the field of cryptography Shows you how to build cryptography into products from the start Examines updates and changes to cryptography Includes coverage on key servers, message security, authentication codes, new standards, block ciphers, message authentication codes, and more Cryptography Engineering gets you up to speed in the ever-evolving field of cryptography.

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World Bruce Schneier 2018-09-04 A world of "smart" devices means the Internet can kill people. We need to act. Now. Everything is a computer. Ovens are computers that make things hot; refrigerators are computers that keep things cold. These computers—from home thermostats to chemical plants—are all online. The Internet, once a virtual abstraction, can now sense and touch the physical world. As we open our lives to this future, often called the Internet of Things, we are beginning to see its enormous potential in ideas like driverless cars, smart cities, and personal agents equipped with their own behavioral algorithms. But every knife cuts two ways. All computers can be hacked. And Internet-connected computers are the most vulnerable. Forget data theft: cutting-edge digital attackers can now crash your car, your pacemaker, and the nation's power grid. In Click Here to Kill Everybody, renowned expert and best-selling author Bruce Schneier examines the hidden risks of this new reality. After exploring the full implications of a world populated by hyperconnected devices, Schneier reveals the hidden web of technical, political, and market forces that underpin the pervasive insecurities of today. He then offers common-sense choices for companies, governments, and individuals that can allow us to enjoy the benefits of this omnipotent age without falling prey to its vulnerabilities. From principles for a more resilient Internet of Things, to a recipe for sane government regulation and oversight, to a better way to understand a truly new environment, Schneier's vision is required reading for anyone invested in human flourishing.

Enforcing Privacy David Wright 2016-04-19 This book is about enforcing privacy and data protection. It demonstrates different approaches – regulatory, legal and technological – to enforcing privacy. If regulators do not enforce laws or regulations or codes or do not have the resources, political support or wherewithal to enforce them, they effectively eviscerate and make meaningless such laws or regulations or codes, no matter how laudable or well-intentioned. In some cases, however, the mere existence of such laws or regulations, combined with a credible threat to invoke them, is sufficient for regulatory purposes. But the threat has to be credible. As some of the authors in this book make clear – it is a theme that runs throughout this book – "carrots" and "soft law" need to be backed up by "sticks" and "hard law". The authors of this book view privacy enforcement as an activity that goes beyond regulatory enforcement, however. In some sense, enforcing privacy is a task that befalls to all of us. Privacy advocates and members of the public can play an important role in combatting the continuing intrusions upon privacy by governments, intelligence agencies and big companies. Contributors to this book - including regulators, privacy advocates, academics, SMEs, a Member of the European Parliament, lawyers and a technology researcher – share their views in the one and only book on Enforcing Privacy.

Cyber Privacy April Falcon Doss 2020-10-20 "Chilling, eye-opening, and timely, Cyber Privacy makes a strong case for the urgent need to reform the laws and policies that protect our personal data. If your reaction to that statement is to shrug your shoulders, think again. As April Falcon Doss expertly explains, data tracking is a real problem that affects every single one of us on a daily basis." —General Michael V. Hayden, USAF, Ret., former Director of CIA and NSA and former Principal Deputy Director of National Intelligence You're being tracked. Amazon, Google, Facebook, governments. No matter who we are or where we go, someone is collecting our data: to profile us, target us, assess us; to predict our behavior and analyze our attitudes; to influence the things we do and buy—even to impact our vote. If this makes you uneasy, it should. We live in an era of unprecedented data aggregation, and it's never been more difficult to navigate the trade-offs between individual privacy, personal convenience, national security, and corporate profits. Technology is evolving quickly, while laws and policies are changing slowly. You shouldn't have to be a privacy expert to understand what happens to your data. April Falcon Doss, a privacy expert and former NSA and Senate lawyer, has seen this imbalance in action. She wants to empower individuals and see policy catch up. In Cyber Privacy, Doss demystifies the digital footprints we leave in our daily lives and reveals how our data is being used—sometimes against us—by the private sector, the government, and even our employers and schools. She explains the trends in data science, technology, and the law that impact our everyday privacy. She tackles big questions: how data aggregation undermines personal autonomy, how to measure what privacy is worth, and how society can benefit from big data while managing its risks and being clear-eyed about its cost. It's high time to rethink notions of privacy and what, if anything, limits the power of those who are constantly watching, listening, and learning about us. This book is for readers who want answers to three questions: Who has your data? Why should you care? And most important, what can you do about it?

Protect Your Macintosh Bruce Schneier 1994-01 Uncovers a host of problems and suggested solutions for issues ranging from protecting data from thieves or spies; backing up and storing files; and safeguarding from viruses to choosing bars, chains, and locks to prevent physical removal. Original. (All Users).

Beyond Fear Bruce Schneier 2006-05-10 Many of us, especially since 9/11, have become personally concerned about issues of security, and this is no surprise. Security is near the top of government and corporate agendas around the globe. Security-related stories appear on the front page everyday. How well though, do any of us truly understand what achieving real security involves? In Beyond Fear, Bruce Schneier invites us to take a critical look at not just the threats to our security, but the ways in which we're encouraged to think about security by law enforcement agencies, businesses of all shapes and sizes, and our national governments and militaries. Schneier believes we all can and should be better security consumers, and that the trade-offs we make in the name of security - in terms of cash outlays, taxes, inconvenience, and diminished freedoms - should be part of an ongoing negotiation in our personal, professional, and civic lives, and the subject of an open and informed national discussion. With a well-deserved reputation for original and sometimes iconoclastic thought, Schneier has a lot to say that is provocative, counter-intuitive, and just plain good sense. He explains in detail, for example, why we need to design security systems that don't just work well, but fail well, and why secrecy on the part of government often undermines security. He also believes, for instance, that national ID cards are an exceptionally bad idea: technically unsound, and even destructive of security. And, contrary to a lot of current nay-sayers, he thinks online shopping is fundamentally safe, and that many of the new airline security measure (though by no means all) are actually quite effective. A skeptic of much that's promised by highly touted technologies like biometrics, Schneier is also a refreshingly positive, problem-solving force in the often self-dramatizing and fear-mongering world of security pundits. Schneier helps the reader to understand the issues at stake, and how to best come to one's own conclusions, including the vast infrastructure we already have in place, and the vaster systems--some useful, others useless or worse--that we're being asked to submit to and pay for. Bruce Schneier is the author of seven books, including Applied Cryptography (which Wired called "the one book the National Security Agency wanted never to be published") and Secrets and Lies (described in Fortune as "startlingly lively...¦[a] jewel box of little surprises you can actually use."). He is also Founder and Chief Technology Officer of Counterpane Internet Security, Inc., and publishes Crypto-Gram, one of the most widely read newsletters in the field of online security.

Do the Work! Steven Pressfield 2014-10-28

The Cybersecurity Dilemma Ben Buchanan 2017-02-01 Why do nations break into one another's most important computer networks? There is an obvious answer: to steal valuable information or to attack. But this isn't the full story. This book draws on often-overlooked documents leaked by Edward Snowden, real-world case studies of cyber operations, and policymaker perspectives to show that intruding into other countries' networks has enormous defensive value as well. Two nations, neither of which seeks to harm the other but neither of which trusts the other, will often find it prudent to launch intrusions. This general problem, in which a nation's means of securing itself threatens the security of others and risks escalating tension, is a bedrock concept in international relations and is called the 'security dilemma'. This book shows not only that the security dilemma applies to cyber operations, but also that the particular characteristics of the digital domain mean that the effects are deeply pronounced. The cybersecurity dilemma is both a vital concern of modern statecraft and a means of accessibly understanding the essential components of cyber operations.

Serious Cryptography Jean-Philippe Aumasson 2017-11-06 This practical guide to modern encryption breaks down the fundamental mathematical concepts at the heart of cryptography without shying away from meaty discussions of how they work. You'll learn about authenticated encryption, secure randomness, hash functions, block ciphers, and public-key techniques such as RSA and elliptic curve cryptography. You'll also learn: - Key concepts in cryptography, such as computational security, attacker models, and forward secrecy - The strengths and limitations of the TLS protocol behind HTTPS secure websites - Quantum computation and post-quantum cryptography - About various vulnerabilities by examining numerous code examples and use cases - How to choose the best algorithm or protocol and ask vendors the right questions Each chapter includes a discussion of common implementation mistakes using real-world examples and details what could go wrong and how to avoid these pitfalls. Whether you're a seasoned practitioner or a beginner looking to dive into the field, Serious Cryptography will provide a complete survey of modern encryption and its applications.

The Good Drone Austin Choi-Fitzpatrick 2020-07-28 How small-scale drones, satellites, kites, and balloons are used by social movements for the greater good. Drones are famous for doing bad things: weaponized, they implement remote-control war; used for surveillance, they

threaten civil liberties and violate privacy. In The Good Drone, Austin Choi-Fitzpatrick examines a different range of uses: the deployment of drones for the greater good. Choi-Fitzpatrick analyzes the way small-scale drones--as well as satellites, kites, and balloons--are used for a great many things, including documenting human rights abuses, estimating demonstration crowd size, supporting anti-poaching advocacy, and advancing climate change research. In fact, he finds, small drones are used disproportionately for good; nonviolent prosocial uses predominate.

Data and Goliath Bruce Schneier 2015-03-02 You are under surveillance right now. Your cell phone provider tracks your location and knows who's with you. Your online and in-store purchasing patterns are recorded, and reveal if you're unemployed, sick, or pregnant. Your e-mails and texts expose your intimate and casual friends. Google knows what you're thinking because it saves your private searches. Facebook can determine your sexual orientation without you ever mentioning it. The powers that surveil us do more than simply store this information. Corporations use surveillance to manipulate not only the news articles and advertisements we each see, but also the prices we're offered. Governments use surveillance to discriminate, censor, chill free speech, and put people in danger worldwide. And both sides share this information with each other or, even worse, lose it to cybercriminals in huge data breaches. Much of this is voluntary: we cooperate with corporate surveillance because it promises us convenience, and we submit to government surveillance because it promises us protection. The result is a mass surveillance society of our own making. But have we given up more than we've gained? In Data and Goliath, security expert Bruce Schneier offers another path, one that values both security and privacy. He shows us exactly what we can do to reform our government surveillance programs and shake up surveillance-based business models, while also providing tips for you to protect your privacy every day. You'll never look at your phone, your computer, your credit cards, or even your car in the same way again.

They Know Everything About You Robert Scheer 2015-02-24 They Know Everything About You is a groundbreaking exposé of how government agencies and tech corporations monitor virtually every aspect of our lives, and a fierce defense of privacy and democracy. The revelation that the government has access to a vast trove of personal online data demonstrates that we already live in a surveillance society. But the erosion of privacy rights extends far beyond big government. Intelligence agencies such as the NSA and CIA are using Silicon Valley corporate partners as their data spies. Seemingly progressive tech companies are joining forces with snooping government agencies to create a brave new world of wired tyranny. Life in the digital age poses an unprecedented challenge to our constitutional liberties, which guarantee a wall of privacy between the individual and the government. The basic assumption of democracy requires the ability of the individual to experiment with ideas and associations within a protected zone, as secured by the Constitution. The unobserved moment embodies the most basic of human rights, yet it is being squandered in the name of national security and consumer convenience. Robert Scheer argues that the information revolution, while a source of public enlightenment, contains the seeds of freedom's destruction in the form of a surveillance state that exceeds the wildest dream of the most ingenious dictator. The technology of surveillance, unless vigorously resisted, represents an existential threat to the liberation of the human spirit.

Obfuscation Finn Brunton 2016-09-02 How we can evade, protest, and sabotage today's pervasive digital surveillance by deploying more data, not less—and why we should. With Obfuscation, Finn Brunton and Helen Nissenbaum mean to start a revolution. They are calling us not to the barricades but to our computers, offering us ways to fight today's pervasive digital surveillance—the collection of our data by governments, corporations, advertisers, and hackers. To the toolkit of privacy protecting techniques and projects, they propose adding obfuscation: the deliberate use of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects. Brunton and Nissenbaum provide tools and a rationale for evasion, noncompliance, refusal, even sabotage—especially for average users, those of us not in a position to opt out or exert control over data about ourselves. Obfuscation will teach users to push back, software developers to keep their user data safe, and policy makers to gather data without misusing it. Brunton and Nissenbaum present a guide to the forms and formats that obfuscation has taken and explain how to craft its implementation to suit the goal and the adversary. They describe a series of historical and contemporary examples, including radar chaff deployed by World War II pilots, Twitter bots that hobbled the social media strategy of popular protest movements, and software that can camouflage users' search queries and stymie online advertising. They go on to consider obfuscation in more general terms, discussing why obfuscation is necessary, whether it is justified, how it works, and how it can be integrated with other privacy practices and technologies.

Dawn of the Code War John P. Carlin 2018-10-16 The inside story of how America's enemies launched a cyber war against us-and how we've learned to fight back With each passing year, the internet-linked attacks on America's interests have grown in both frequency and severity. Overmatched by our military, countries like North Korea, China, Iran, and Russia have found us vulnerable in cyberspace. The "Code War" is upon us. In this dramatic book, former Assistant Attorney General John P. Carlin takes readers to the front lines of a global but little-understood fight as the Justice Department and the FBI chases down hackers, online terrorist recruiters, and spies. Today, as our entire economy goes digital, from banking to manufacturing to transportation, the potential targets for our enemies multiply. This firsthand account is both a remarkable untold story and a warning of dangers yet to come.

The Aisles Have Eyes Joseph Turow 2017-01-17 The author of Media Today offers "a trenchant, timely, and troubling account of [retailers'] data-mining, in-store tracking, and predictive analytics" (The Philadelphia Inquirer). By one expert's prediction, within twenty years half of Americans will have body implants that tell retailers how they feel about specific products as they browse their local stores. The notion may be outlandish, but it reflects executives' drive to understand shoppers in the aisles with the same obsessive detail that they track us online. In fact, a hidden surveillance revolution is already taking place inside brick-and-mortar stores, where Americans still do most of their buying. Drawing on his interviews with retail executives, analysis of trade publications, and experiences at insider industry meetings, advertising and digital studies expert Joseph Turow pulls back the curtain on these trends, showing how a new hyper-competitive generation of merchants—including Macy's, Target, and Walmart—is already using data mining, in-store tracking, and predictive analytics to change the way we buy, undermine our privacy, and define our reputations. Eye-opening and timely, Turow's book is essential reading to understand the future of shopping. "Turow shows shopping today to be an exercise in unwitting self-revelation—and not only online."—The Wall Street Journal "Thoroughly researched and clearly presented with detailed evidence and fascinating peeks inside the retail industry. Much of this information is startling and even chilling, particularly when Turow shows how retail data-tracking can enable discrimination and societal stratification."—Publishers Weekly "Revealing . . . Valuable reading for shoppers and retailers alike."—Kirkus Reviews

Hands-On Cryptography with Python Samuel Bowne 2018-06-29 Learn to evaluate and compare data encryption methods and attack cryptographic systems Key Features Explore popular and important cryptographic methods Compare cryptographic modes and understand their limitations Learn to perform attacks on cryptographic systems Book Description Cryptography is essential for protecting sensitive information, but it is often performed inadequately or incorrectly. Hands-On Cryptography with Python starts by showing you how to encrypt and evaluate your data. The book will then walk you through various data encryption methods,such as obfuscation, hashing, and strong encryption, and will show how you can attack cryptographic systems. You will learn how to create hashes, crack them, and will understand why they are so different from each other. In the concluding chapters, you will use three NIST-recommended systems: the Advanced Encryption Standard (AES), the Secure Hash Algorithm (SHA), and the Rivest-Shamir-Adleman (RSA). By the end of this book, you will be able to deal with common errors in encryption. What you will learn Protect data with encryption and hashing Explore and compare various encryption methods Encrypt data using the Caesar Cipher technique Make hashes and crack them Learn how to use three NIST-recommended systems: AES, SHA, and RSA Understand common errors in encryption and exploit them Who this book is for Hands-On Cryptography with Python is for security professionals who want to learn to encrypt and evaluate data, and compare different encryption methods.

Secrets and Lies Bruce Schneier 2015-03-23 This anniversary edition which has stood the test of time as a runaway best-seller provides a practical, straight-forward guide to achieving security throughout computer networks. No theory, no math, no fiction of what should be working but isn't, just the facts. Known as the master of cryptography, Schneier uses his extensive field experience with his own clients to dispel the myths that often mislead IT managers as they try to build secure systems. A much-touted section: Schneier's tutorial on just what cryptography (a subset of computer security) can and cannot do for them, has received far-reaching praise from both the technical and business community. Praise for Secrets and Lies "This is a business issue, not a technical one, and executives can no longer leave such decisions to techies. That's why Secrets and Lies belongs in every manager's library."-Business Week "Startlingly lively....a jewel box of little surprises you can actually use."-Fortune "Secrets is a comprehensive, well-written work on a topic few business leaders can afford to neglect."-Business 2.0 "Instead of talking algorithms to geeky programmers, [Schneier] offers a primer in practical computer security aimed at those shopping, communicating or doing business online-almost everyone, in other words."-The Economist "Schneier...peppers the book with lively anecdotes and aphorisms, making it unusually accessible."-Los Angeles Times With a new and compelling Introduction by the author, this premium edition will become a keepsake for security enthusiasts of every stripe.

Fukushima David Lochbaum 2015-02-10 "A gripping, suspenseful page-turner" (Kirkus Reviews) with a "fast-paced, detailed narrative that moves like a thriller" (International Business Times), Fukushima teams two leading experts from the Union of Concerned Scientists, David Lochbaum and Edwin Lyman, with award-winning journalist Susan Q. Stranahan to give us the first definitive account of the 2011 disaster that led to the worst nuclear catastrophe since Chernobyl. Four years have passed since the day the world watched in horror as an earthquake large enough to shift the Earth's axis by several inches sent a massive tsunami toward the Japanese coast and Fukushima Daiichi nuclear power plant, causing the reactors' safety systems to fail and explosions to reduce concrete and steel buildings to rubble. Even as the consequences of the 2011 disaster continue to exact their terrible price on the people of Japan and on the world, Fukushima addresses the grim questions at the heart of the nuclear debate: could a similar catastrophe happen again, and—most important of all—how can such a crisis be averted?

Dark Mirror Barton Gellman 2020-05-19 From the three-time Pulitzer Prize-winning author of the New York Times bestseller Angler, who unearthed the deepest secrets of Edward Snowden's NSA archive, the first master narrative of the surveillance state that emerged after 9/11 and why it matters, based on scores of hours of conversation with Snowden and groundbreaking reportage in Washington, London, Moscow and Silicon Valley Edward Snowden chose three journalists to tell the stories in his Top Secret trove of NSA documents: Barton Gellman of The Washington Post, Glenn Greenwald of The Guardian and filmmaker Laura Poitras, all of whom would share the Pulitzer Prize for Public Service. Poitras went on to direct the Oscar-winning Citizen Four. Greenwald wrote an instant memoir and cast himself as a pugilist on Snowden's behalf. Barton Gellman took his own path. Snowden and his documents were the beginning, not the end, of a story he had prepared his whole life to tell. More than 20 years as a top investigative journalist armed him with deep sources in national security and high technology. New sources reached out from government and industry, making contact on the same kinds of secret, anonymous channels that Snowden used. Gellman's old reporting notes unlocked new puzzles in the NSA archive. Long days and evenings with Snowden in Moscow revealed a complex character who fit none of the stock images imposed on him by others. Gellman now brings his unique access and storytelling gifts to a true-life spy tale that touches us all. Snowden captured the public imagination but left millions of people unsure what to think. Who is the man, really? How did he beat the world's most advanced surveillance agency at its own game? Is government and corporate spying as bad as he says? Dark Mirror is the master narrative we have waited for, told with authority and an inside view of extraordinary events. Within it is a personal account of the obstacles facing the author, beginning with Gellman's discovery of his own name in the NSA document trove. Google notifies him that a foreign government is trying to compromise his account. A trusted technical adviser finds anomalies on his laptop. Sophisticated impostors approach Gellman with counterfeit documents, attempting to divert or discredit his work. Throughout Dark Mirror, the author describes an escalating battle against unknown digital adversaries, forcing him to mimic their tradecraft in self-defense. Written in the vivid scenes and insights that marked Gellman's bestselling Angler, Dark Mirror is an inside account of the surveillance-industrial revolution and its discontents, fighting back against state and corporate intrusions into our most private spheres. Along the way it tells the story of a government leak unrivaled in drama since All the President's Men.