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

As recognized, adventure as capably as experience nearly lesson, amusement, as well as deal can be gotten by just checking out a ebook **Data And Goliath The Hidden Battles To Collect Your Data And Control Your World** as well as it is not directly done, you could agree to even more almost this life, with reference to the world.

We allow you this proper as capably as simple habit to acquire those all. We offer Data And Goliath The Hidden Battles To Collect Your Data And Control Your World and numerous book collections from fictions to scientific research in any way. in the middle of them is this Data And Goliath The Hidden Battles To Collect Your Data And Control Your World that can be your partner.

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.

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"--

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.

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.

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 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.

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."

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.

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.

Dark Mirror Barton Gellman 2021-05-18 “Engrossing. . . . Gellman [is] a thorough, exacting reporter . . . a marvelous narrator for this particular story, as he nimbly guides us through complex technical arcana and some stubborn ethical questions. . . . Dark Mirror would be simply pleasurable to read if the story it told didn’t also happen to be frighteningly real.” —Jennifer Szalai, The New York Times From the three-time Pulitzer Prize winner and author of the New York Times bestseller Angler, the definitive master narrative of Edward Snowden and the modern surveillance state, based on unique access to Snowden and groundbreaking reportage around the world. Edward Snowden touched off a global debate in 2013 when he gave Barton Gellman, Laura Poitras and Glenn Greenwald each a vast and explosive archive of highly classified files revealing the extent of the American government’s access to our every communication. They shared the Pulitzer Prize that year for public service. For Gellman, who never stopped reporting, that was only the beginning. He jumped off from what Snowden gave him to track the reach and methodology of the U.S. surveillance state and bring it to light with astonishing new clarity. Along the way, he interrogated Snowden’s own history and found important ways in which myth and reality do not line up. Gellman treats Snowden with respect, but this is no hagiographic account, and Dark Mirror sets the record straight in ways that are both fascinating and important. Dark Mirror is the story that Gellman could not tell before, a gripping inside narrative of investigative reporting as it happened and a deep dive into the machinery of the surveillance state. Gellman recounts the puzzles, dilemmas and tumultuous events behind the scenes of his work — in top secret intelligence facilities, in Moscow hotel rooms, in huddles with Post lawyers and editors, in Silicon Valley executive suites, and in encrypted messages from anonymous accounts. Within the book is a compelling portrait of national security journalism under pressure from legal threats, government investigations, and foreign intelligence agencies intent on stealing Gellman’s files. Throughout Dark Mirror, Gellman wages an escalating battle against unknown adversaries who force him to mimic their tradecraft in self-defense. With the vivid and insightful style that is the author’s trademark, Dark Mirror is a true-life spy tale about the surveillance-industrial revolution and its discontents. Along the way, with the benefit of fresh reporting, it tells the full story of a government leak unrivaled in drama since All the President’s Men.

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.

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.

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.

Windows Into the Soul Gary T. Marx 2016-05-31 In Windows into the Soul, Gary T. Marx sums up a lifetime of work on issues of surveillance and social control by disentangling and parsing the empirical richness of watching and being watched. Ultimately, Marx argues, recognizing complexity and asking the right questions is essential to bringing light and accountability to the darker, more iniquitous corners of our emerging surveillance society.

Do the Work! Steven Pressfield 2014-10-28

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.

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.

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?

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

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).

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.

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?

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.

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.

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.

Book Wars John B. Thompson 2021-03-04 This book tells the story of the turbulent decades when the book publishing industry collided with the great technological revolution of our time. From the surge of ebooks to the self-publishing explosion and the growing popularity of audiobooks, Book Wars provides a comprehensive and fine-grained account of technological disruption in one of our most important and

successful creative industries. Like other sectors, publishing has been thrown into disarray by the digital revolution. The foundation on which this industry had been based for 500 years – the packaging and sale of words and images in the form of printed books – was called into question by a technological revolution that enabled symbolic content to be stored, manipulated and transmitted quickly and cheaply. Publishers and retailers found themselves facing a proliferation of new players who were offering new products and services and challenging some of their most deeply held principles and beliefs. The old industry was suddenly thrust into the limelight as bitter conflicts erupted between publishers and new entrants, including powerful new tech giants who saw the world in very different ways. The book wars had begun. While ebooks were at the heart of many of these conflicts, Thompson argues that the most fundamental consequences lie elsewhere. The print-on-paper book has proven to be a remarkably resilient cultural form, but the digital revolution has transformed the industry in other ways, spawning new players which now wield unprecedented power and giving rise to an array of new publishing forms. Most important of all, it has transformed the broader information and communication environment, creating new challenges and new opportunities for publishers as they seek to redefine their role in the digital age. This unrivalled account of the book publishing industry as it faces its greatest challenge since Gutenberg will be essential reading for anyone interested in books and their future.

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.

Nothing to Hide Daniel J. Solove 2011-05-31 "If you've got nothing to hide," many people say, "you shouldn't worry about government surveillance." Others argue that we must sacrifice privacy for security. But as Daniel J. Solove argues in this important book, these arguments and many others are flawed. They are based on mistaken views about what it means to protect privacy and the costs and benefits of doing so. The debate between privacy and security has been framed incorrectly as a zero-sum game in which we are forced to choose between one value and the other. Why can't we have both? In this concise and accessible book, Solove exposes the fallacies of many pro-security arguments that have skewed law and policy to favor security at the expense of privacy. Protecting privacy isn't fatal to security measures; it merely involves adequate oversight and regulation. Solove traces the history of the privacy-security debate from the Revolution to the present day. He explains how the law protects privacy and examines concerns with new technologies. He then points out the failings of our current system and offers specific remedies. Nothing to Hide makes a powerful and compelling case for reaching a better balance between privacy and security and reveals why doing so is essential to protect our freedom and democracy"--Jacket.

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.

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.

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.

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.

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.

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?

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?

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.

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

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.

Janesville Amy Goldstein 2017-04-18 * Financial Times and McKinsey Business Book of the Year * Winner of the J. Anthony Lukas Book Prize * 800-CEO-READ Business Book of the Year * A New York Times Notable Book * A Washington Post Notable Book * An NPR Best Book of 2017 * A Wall Street Journal Best Book of 2017 * An Economist Best Book of 2017 * A Business Insider Best Book of 2017 * “A gripping story of psychological defeat and resilience” (Bob Woodward, The Washington Post)—an intimate account of the fallout from the closing of a General Motors assembly plant in Janesville, Wisconsin, and a larger story of the hollowing of the American middle class. This is the story of what happens to an industrial town in the American heartland when its main factory shuts down—but it’s not the familiar tale. Most observers record the immediate shock of vanished jobs, but few stay around long enough to notice what happens next when a community with a can-do spirit tries to pick itself up. Pulitzer Prize–winning reporter Amy Goldstein spent years immersed in Janesville, Wisconsin, where the nation’s oldest operating General Motors assembly plant shut down in the midst of the Great Recession. Now, with intelligence, sympathy, and insight into what connects and divides people in an era of economic upheaval, Goldstein shows the consequences of one of America’s biggest political issues. Her reporting takes the reader deep into the lives of autoworkers, educators, bankers, politicians, and job re-trainers to show why it’s so hard in the twenty-first century to recreate a healthy, prosperous working class. “Moving and magnificently well-researched...Janesville joins a growing family of books about the evisceration of the working class in the United States. What sets it apart is the sophistication of its storytelling and analysis” (Jennifer Senior, The New York Times). “Anyone tempted to generalize about the American working class ought to meet the people in Janesville. The reporting behind this book is extraordinary and the story—a stark, heartbreaking reminder that political ideologies have real consequences—is told with rare sympathy and insight” (Tracy Kidder, Pulitzer Prize–winning author of The Soul of a New Machine).

E-mail Security Bruce Schneier 1995-01-25 A non-technical approach to the issue of privacy in E-Mail rates the security of popular programs and offers practical solutions--two leading-edge encryption programs, PEM (Privacy Enhanced Mail) and PGP (Pretty Good Privacy). Original. (All Users).