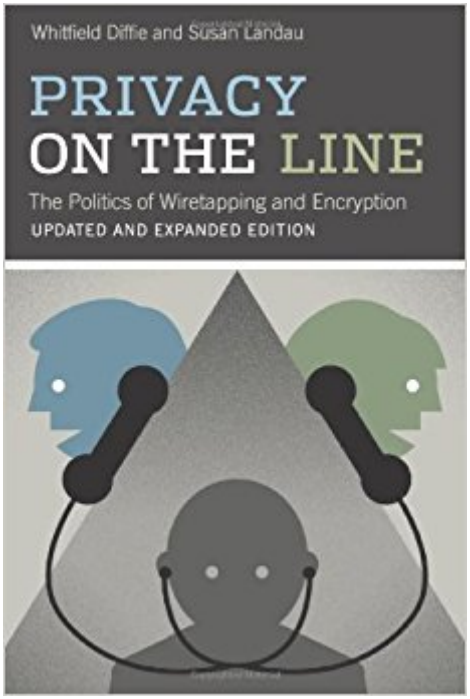
Privacy On The Line: The Politics Of Wiretapping And Encryption (MIT Press)



Synopsis

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

Book Information

Series: MIT Press

Hardcover: 496 pages

Publisher: The MIT Press; updated and expanded edition edition (March 30, 2007)

Language: English

ISBN-10: 0262042401

ISBN-13: 978-0262042406

Product Dimensions: 6 x 1.1 x 9 inches

Shipping Weight: 1.8 pounds (View shipping rates and policies)

Average Customer Review: 5.0 out of 5 stars 3 customer reviews

Best Sellers Rank: #1,084,074 in Books (See Top 100 in Books) #99 inÃ Â Books > Law > Intellectual Property > Communications #326 inÃ Â Books > Computers & Technology > Computer Science > Information Theory #717 inÃ Â Books > Textbooks > Social Sciences > Political Science > Civil Rights

Customer Reviews

A compact and intelligible guide to both the technical and the political issues. (Laurence A. Marschall The Sciences)A superb and timely introduction to a subject of enormous importance for scholars and citizens alike. (Choice)A well-researched and fascinating study. (Lawrence Rothstein Law and Politics Review)A wise, meticulously researched guide.... (London Review of Books)An incredibly comprehensive insight into the world of encryption and wiretaps, its political machinations, legal aspects, technologies, vulnerabilities, costs, limitations, and near-ubiquity. (G. Ernest Govea Security Management)Diffie and Landau deserve a large audience. Their lucid exposition adds valuable context to debates that for too long have been abstract. (Aziz Huq The American Prospect)Should be required reading for any computing student at any level. (Harold Thimbleby New Scientist)The book details numerous privacy issues, from personal privacy to national security.... A welcome surprise is that the book often reads like a Tom Clancy novel, interwoven as it is with episodes of domestic and international intrigue.... A timely and important book. (Ben Rothke Security Management)A superb and timely introduction to a subject of enormous importance for scholars and citizens alike. (Choice)[A] wise, meticulously researched guide... (London Review of Books)

Whitfield Diffie, the inventor of public-key cryptography, is Visiting Professor at Royal Holloway College at the Universityof London.Susan Landau is a privacy analyst at Google. She was previously a Distinguished Engineer at Sun Microsystems, and has been a faculty member at the University of Massachusetts at Amherst and at Wesleyan University. Landau has been a Guggenheim fellow, a fellow at the Radcliffe Institute for Advanced Study, and is a fellow of the American Association for the advancement of Science and the Association for Computing Machinery.

After hearing the 2013 news reports about U.S. government surveillance, I wanted to get more informed on the issues.I had no idea that government surveillance has been as pervasive as it is, for as long as it has been. We learn here of privacy violations starting at least in the late 1800s in the form of overreaching census taking; numerous people were arrested for refusing to answer questions that they thought were none of the government’s business to be asking.The book takes us from there through about 2005 (published in 2007), with accounts of excessive wiretapping on Martin Luther King Jr., opening the mail of private citizens, increasingly extending the reach of authorized wiretapping, attempting to learn from the public library system who might be a spy based on checking out books about science, and more.This isn’t light reading, with an immense amount of

information conveyed, but if you're interested in learning more about privacy and surveillance in the United States, this is an excellent resource.

I bought this book while taking a graduate course in Cryptography for a research paper on privacy and encryption. The field is rather fascinating and this book does an excellent job of providing the whys for some of the recent legislation. Anyone who is concerned about social networking Internet sites and Internet privacy should read this book. It uses no scare tactics or big brother is watching you drama, it is based on research and facts and presents the current state of affairs in privacy in a professional manner. Whitfield Diffie has been instrumental in helping to bring the field of Cryptanalysis from a linguist-based discipline to a mathematical one (Diffie-Hellman symmetric encryption key exchange or Alice & Bob exchanging secure messages examples) and this book is a logical extension of his craft. I found it chock full of information I did not know about how the concept of privacy has evolved and with it the evolving legislation. If you are aware of the Electronic Frontier Foundation's lawsuits regarding the unethical (and for At&T unlawful) surveillance (capture of data) of American citizens and just about anyone who has a computer or a cell phone by the commiseration of NSA and At&T in San Francisco, CA, it would help if you read this book to understand how we reached these new heights in the invasion of personal privacy and introduce you to cryptography's role in it. Highly recommend.

Unfortunately the book starts with a bad impression by confusing Constitutional Amendment IV with Article IV. After getting over the mis-impression it's clear that this is the best available on mechanics, history and politics of encryption.The book features an expert analysis of the features and advantages of public key encryption with the politics of key escrow. In it's detailed examination of all aspects, the book considers cost/benefit analysis. Written in 1998, the book could stand updating for technology improvements and recent legislation.I'm convinced that encryption is not necessary for law enforcement. I'm not so sure about data security. The main issue is who should handle it. D&L point out that the NSA is winning its turf war with NIST. I doubt that Apple and Google can hold their ground for very long. I'm afraid that the issue might be moot as control will inevitable accrue to the government.This effort is as informative as possible in a book that is nearing 20 years old, a long time for the rate of today's technology development. I would be the first to read a second edition. Note: Now I understand that a second edition was published in 2007. I guess I won't be the first to read it.

Privacy on the Line: The Politics of Wiretapping and Encryption (MIT Press) Obfuscation: A User's Guide for Privacy and Protest (MIT Press) Facebook Safety and Privacy (21st Century Safety and Privacy) Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age (2nd Edition) Online Privacy and Social Media (Privacy in the Online World) Approaches to Solve Big Data Security Issues and Comparative Study of Cryptographic Algorithms for Data Encryption ISO/IEC 18033-2:2006, Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers The Mathematics of Secrets: Cryptography from Caesar Ciphers to Digital Encryption Mastering Algorithms with C: Useful Techniques from Sorting to Encryption The End of Privacy: The Attack on Personal Rights at Home, at Work, On-Line, and in Court What a City Is For: Remaking the Politics of Displacement (MIT Press) Lerne FranzÃƒÂ¶sisch mit Mimi: Mimi und die Ausstellung. Ein Bilderbuch auf FranzÃƒÂ¶sisch/Deutsch mit Vokabeln (Mimi de-fr 2) (German Edition) Lies Mit Mir! Intermediate Reader 2 (Komm Mit) Komm mit!: Beginner Reader Lies mit mir Level 1 Komm mit!: Advanced Reader Lies mit mir Level 3 Komm mit! German: PRAC & ACT BK KOMM MIT! HOLT GERMAN 2 95 Level 2 Westafrika mit dem Fahrrad: Mit dem Rad durch Marokko, Mauretanien, Senegal, Mali, Burkina Faso und Togo (German Edition) Botanical Line Drawing: 200+ Step by Step Drawings of Trees, Flowers, Fruits, Leaves and Vegetables: The Complete Workbook of Botanical Line Drawing LINE OF CREDIT: Line Of Credit Secrets Revealed For Your Business, Equity And Taxes Clothing Line Start-Up Secrets: How to Start and Grow a Successful Clothing Line