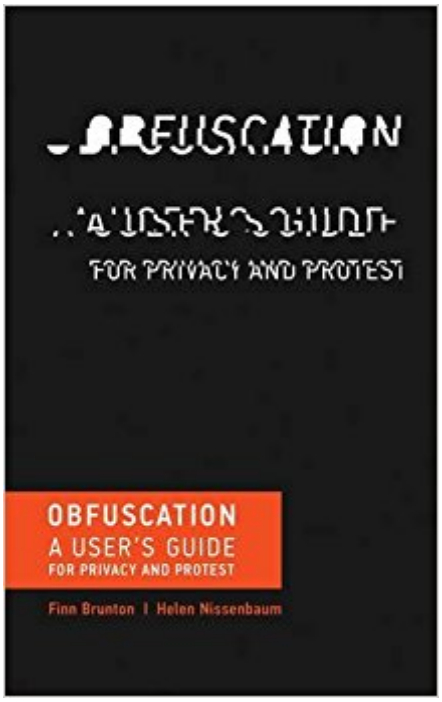
Ebook Directory
the best source of ebook

The book was found

Obfuscation: A User's Guide For Privacy And Protest (MIT Press)



PDF
Adobe
DOWNLOAD EBOOK

Synopsis

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.

Book Information

Series: MIT Press

Paperback: 136 pages

Publisher: The MIT Press; Reprint edition (September 2, 2016)

Language: English

ISBN-10: 0262529866

ISBN-13: 978-0262529860

Product Dimensions: 5 x 0.4 x 8 inches

Shipping Weight: 4.8 ounces (View shipping rates and policies)

Average Customer Review: 4.0 out of 5 stars 15 customer reviews

Best Sellers Rank: #159,651 in Books (See Top 100 in Books) #16 inÃ Â Books > Politics & Social Sciences > Social Sciences > Privacy & Surveillance #91 inÃ Â Books > Computers & Technology > Security & Encryption > Privacy & Online Safety #396 inÃ Â Books > Computers & Technology > Networking & Cloud Computing > Internet, Groupware, & Telecommunications

Customer Reviews

By mapping out obfuscation tools, practices, and goals, Brunton and Nissenbaum provide a valuable framework for understanding how people seek to achieve privacy and control in a data-soaked world. This important book is essential for anyone trying to understand why people resist and challenge tech norms, including policymakers, engineers, and users of technology (danah boyd, author of It's Complicated: The Social Lives of Networked Teens and founder of Data & Society) Obfuscation is an intelligently written handbook for subversives. I found the historical examples fascinating and the ethical discussion thought-provoking. (Lorrie Faith Cranor, Director, CyLab Usable Privacy and Security Laboratory, Carnegie Mellon University)This book presents a fascinating collection of examples of decoys, camouflage, and information hiding from the human and animal worlds, with a discussion of how such techniques can be used in applications from privacy online through search optimization to propaganda and deception. It leads to discussion of informational justice, and the extent to which camouflage can perhaps help people hide in plain sight online. (Ross Anderson, Professor of Security Engineering, Computer Laboratory, University of Cambridge)At Obfuscation's core is a dystopian vision, offering solutions for "users" who are assumed to have enough want-to and know-how to follow the authors down this road. It is a shame that obfuscation to this degree has become necessary. But at least we are now armed with the necessary knowledge, thanks to this book. (Times Higher Education)Right now we're being watched. It might not be literal watching: it might be that a computer somewhere, owned by a government or a corporation, is collecting or mining the crumbs of data we all left around the world today.... When it comes to maintaining their digital privacy, many people probably think about software like encrypted messaging apps and Tor browsers. But as Brunton and Nissenbaum detail in Obfuscation, there are many other ways to hide one's digital trail. Obfuscation, the first book-length look at the topic, contains a wealth of ideas for prankish disobedience, analysis-frustrating techniques, and other methods of collective protest. (Motherboard)

Finn Brunton is Assistant Professor of Media, Culture, and Communication at New York University and the author of Spam: A Shadow History of the Internet (MIT Press. Helen Nissenbaum is Professor of Media, Culture, and Communication and Computer Science at New York University and the author of Privacy in Context. She is one of the developers of the TrackMeNot software.

Perhaps the coolest thing about Obfuscation by Finn Brunton and Helen Nissenbaum is the title. Obfuscation is such a lovely word, illustrating as it does, the very act of obfuscating by using an unfamiliar word. To obfuscate is to obscure ÃƒÂ¢Ã â ¬Ã Å“intended meaning in communication,

making the message confusing, willfully ambiguous, or harder to understandÃƒÂ¢Ã â ¬Ã Â• (Wikipedia) or ÃƒÂ¢Ã â ¬Ã Å“to make something less clear and harder to understand, especially intentionallyÃƒÂ¢Ã â ¬Ã Â• (Cambridge free online dictionary).This book is about ways of obfuscating and why to obfuscate, particularly in the context of digital collection of personal data and the lack of privacy that ensues.The first third of the book (Part One) is devoted to examples of obfuscation both in digital contexts and in other contexts. This is probably the most useful part of the book in that it provides a catalogue of obfuscatory activities that helps in analysing their nature. Having a set of examples makes it possible to see patterns in the types of activities, their goals and the resources that need to be brought to bear.The next third of the book (Part Two) provides an argument for obfuscation as a legitimate and morally defensible activity, particularly in the context of a world where we are often ÃƒÂ¢Ã â ¬Ã Å“unable to refuse or deny observationÃƒÂ¢Ã â ¬Ã Â•. If people cannot escape being watched in the digital world, usually by those in positions of power, then individual actions as well as the creation of tools to obfuscate is a reasonable response. I found the argument for obfuscation convincing, but then I have long been in the habit of entering bogus phone numbers in those books that must be signed to gain access to buildings. The discussion of ethics, although the densest part of the book, is also useful in that it sets out the arguments clearly enough to be followed with a bit of effort.The authors are both based at New York University. Finn Brunton, on his web page, describes his work thus: ÃƒÂ¢Ã â ¬Ã Å“I work on the history and theory of digital media technology, with a focus on adoption: how computing and networking machinery gets adapted, abused, modified, hacked, and transformed. I want to understand how we can use digital technologies to build a more equitable, just, decentralized, experimental and interesting society.ÃƒÂ¢Ã â ¬Ã Â• I like the way he describes the kind of society that he wants to build. I could buy into that. Helen Nissenbaum has an illustrious profile and her own Wikipedia entry, with research focused on security and privacy in the online world. What I learned from trawling her profile is that her undergraduate degrees are from the University of the Witwatersrand in Johannesburg, where I work.What I particularly like (being an academic) is that almost one third of the book (the last third) is taken up with endnotes ÃƒÂ¢Ã â ¬Ã â œ lots of lovely links to explore the details of each example, and the arguments presented. I will have fun exploring some of those. I plan to use the book with my MasterÃƒÂ¢Ã â ¬Ã â„¢s class in 2016 since a discussion of privacy issues forms part of the Trends in Information Systems course which I teach. I think it will be a good starting point from which to explore.My one disappointment with the book is that I was hoping for more direct advice to me as an individual as to which obfuscating activities I can, or ought to, take part in. The book is actually aimed more at someone designing software or some other

ÃƒÂ¢Ã â ¬Ã Å“programÃƒÂ¢Ã â ¬Ã Â• of resistance. The opening line promises to ÃƒÂ¢Ã â ¬Ã Å“start a revolutionÃƒÂ¢Ã â ¬Ã Â•. I was left eager to join the barricades, but not quite sure where to find them. Perhaps an individualÃƒÂ¢Ã â ¬Ã â„¢s guide will follow?

I bought this book really wanting to love it, and luckily I did.Overall it is a light and breezy read, less than 100 pages in length. The arguments the book presents are straightforward, and while often boiling down to "It depends", the authors do make a good effort to explain what it depends upon. The language used in the book is clear and accessible, not requiring frequent trips to the dictionary. The sadness at quickly arriving at the book's end is offset by the wealth of endnotes and a bibliography that should keep me engaged in the topic for some time.As a call to arms, it might be faulted being a bit meek. But then again, it is about attempting to address an imbalance of power and a lack of polemic maybe it's strength.

This book is an interesting read covering an approach to protecting personal privacy that isn't often discussed. Obfuscation is the act of polluting the data collected such that the collector cannot know which data is correct, and which is bogus. For personal privacy its a way to stop organizations that you interact with from knowing about you e.g. what you are searching about, which web sites you interact with and so on.I found the topic very interesting and worth exploring. However, I did find the writing style a little too wordy and it was laborious to work through the book. Hence my rating of 4 stars.

I would have given 5 stars, but some of the content was too verbose and academic. It was challenging to parse the language at times. But I highly recommended this book especially to technologists and legalists interested in improving privacy in the digital age

Author does a great job writing this book in a way that anyone can understand the concepts that are being presented.

Ok read, just the start I wanted.

Raised some interesting & thought provoking points.Very good read.

Fun and informative.

Download to continue reading...

Obfuscation: A User's Guide for Privacy and Protest (MIT Press) Obfuscation: A User's Guide for Privacy and Protest Windows 10: The Ultimate 2017 Updated User Guide to Microsoft Windows 10 (2017 updated user guide, tips and tricks, user manual, user guide, Windows 10) How to Install Kodi on Firestick: The Ultimate User Guide How to Install Kodi on Fire Stick (the 2017 updated user guide, tips and tricks, home ... (user guides, fire stick,) Echo: Echo Advanced User Guide (2017 Updated) : Step-by-Step Instructions to Enrich your Smart Life (Echo User Manual, Alexa User Guide, Echo Dot, Echo Tap) Echo Dot: Echo Dot User Manual: From Newbie to Expert in One Hour: Echo Dot 2nd Generation User Guide: (Echo, Dot, Echo Dot, ... Manual, Alexa, User Manual, Echo Dot ebook) Privacy on the Line: The Politics of Wiretapping and Encryption (MIT Press) Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age (2nd Edition) Facebook Safety and Privacy (21st Century Safety and Privacy) Online Privacy and Social Media (Privacy in the Online World) Windows 10: The Ultimate 2 in 1 User Guide to Microsoft Windows 10 User Guide to Microsoft Windows 10 for Beginners and Advanced Users (tips and tricks, ... Windows, softwares, guide Book 7) Kindle Fire: Owner's Manual: Ultimate Guide to the Kindle Fire, Beginner's User Guide (User Guide, How to, Hints, Tips and Tricks) Echo: The 2017 Updated Echo User Guide and Echo Dot User Guide, Master Your Echo and Echo Dot in 1 Hour! (With Step-by-Step Instructions & The 250 Best Echo Easter Eggs included) Windows 10: The Best Guide How to Operate New Microsoft Windows 10 (tips and tricks, 2017 user manual, user guide, updated and edited, Windows for beginners) Windows 10: The Best Guide How to Operate New Microsoft Windows 10 (tips and tricks, user manual, user guide, updated and edited, Windows for beginners) How to Install Kodi on Firestick: A Step by Step User Guide How to Install Kodi on Fire Stick (the 2017 updated user guide, tips and tricks, home ... tv, by echo,digital media,internet) A User's Guide to Morning and Evening Prayer (User's Guide to the Book of Common Prayer) Windows 10: Complete Beginners Guide To Microsoft WINDOWS 10 (Tips And Tricks, User Manual, 2017 Updated User Guide) Echo: Master Your Echo; User Guide and Manual (Echo Updated 2017 User Guide) User's Guide to Preventing & Treating Headaches Naturally: Learn How You Can Use Diet and Supplements to Put an End to Headaches (Basic Health Publications User's Guide)

Contact Us

DMCA

Privacy