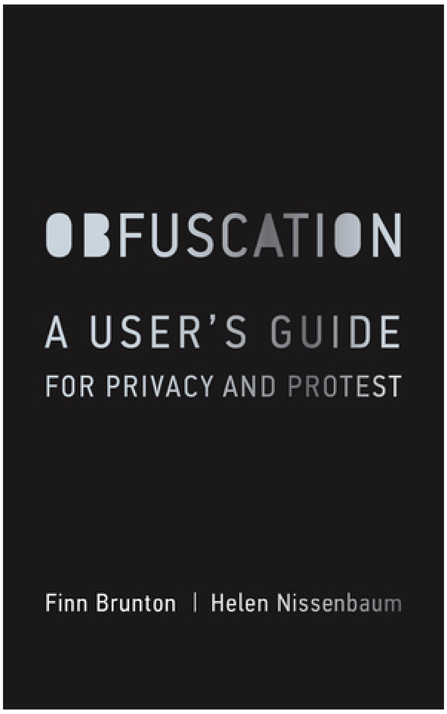

Obfuscation: A User's Guide for Privacy and Protest

Finn Brunton , Helen Nissenbaum

Obfuscation: A User's Guide for Privacy and Protest

Finn Brunton , Helen Nissenbaum

Obfuscation: A User's Guide for Privacy and Protest Finn Brunton , Helen Nissenbaum
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.

Obfuscation: A User's Guide for Privacy and Protest Details

Date	:	Published August 2015 by MIT Press
ISBN	:	9780262029735
Author	:	Finn Brunton , Helen Nissenbaum
Format	:	Hardcover 144 pages
Genre	:	Nonfiction, Science, Technology, Philosophy, Politics

Download and Read Free Online Obfuscation: A User's Guide for Privacy and Protest Finn Brunton , Helen Nissenbaum

From Reader Review Obfuscation: A User's Guide for Privacy and Protest for online ebook

Kelsey Breseman says

Pragmatic, amusing, philosophical, concise. Definitely a book I enjoyed reading overall, but occasionally quite dense in prose.

Nicolas Grasset says

The first chapter are extremely informative and the different sections are very up to date (January 2017). I skipped over the last part around ethics and political motive since it's really not what we want to read from the authors who otherwise managed to focus on a simple read. Most tactics are obvious but some were completely new to me, or the usage examples were. 5* rating because I strongly recommend it, and if we all know about it, obfuscation will work better for the few people who really need it the most: post to Facebook.

Paul says

Title obfuscates the contents. Not a guide. Should be titled: the politics and ethics of obfuscation. Interesting arguments but completely irrelevant to absolutely everyone except academics.

Jay says

Not so much a how-to book, this is more of a why-to, with some examples included that provide some ideas of what-to-do. Many of the examples are from the non-IT world, like radar chaff and the use of common masks or uniforms to temporarily confuse the police in the immediate aftermath of a robbery. But there are also examples of internet-era technology obfuscation, including Twitter-bots hijacking hashtag terms, and services that robotically send out streams of unnecessary searches in order to hide the handful of critical searches in the volume. There is certainly plenty to think about, and the authors do a good job of covering the pros and cons of obfuscation, including ethical considerations. This is one of those books that, although relatively short, will have a continued impact on how I think about obfuscation as a tool for the weak against the powerful, and it points up some additional risks of relying on data for optimization algorithms when that data could have been sabotaged.

In one section, the authors described obfuscation involving colluding people in a group that all claimed a single identity or claimed to be the cause of some action. Ah, I’m thinking, I know of this. Then the authors use as an example a scene from the movie “Spartacus,” where the slaves are asked which one is Spartacus, and all slaves claim to be Spartacus, a group act which saved Spartacus’ life. I found it funny that I was thinking of a movie as well, but it was “Seven Brides for Seven Brothers” to illustrate the same thing the same way. I’m not sure what to make of this, but it strikes me as funny.

Terry says

Decent, but the font was annoying to read and the thread of thought seemed cluttered and the narrative hard to keep cogent at times. Still, I'm glad I read this.

Deane Barker says

This book can only really be described as a manifesto. I don't know what I was expecting really.

It starts by identifying and offering a broad survey of obfuscation methods. And while clearly focused on technology, it discussed other, offline obfuscation: chaff deployed from fighter planes, something the orb-weaving spider does, and even the museum climax scene in "The Thomas Crown Affair." This, I found interesting.

But then the book took a left turn into...philosophy. It spends an inordinate amount of time talking about the philosophy of privacy and offered ethical justification to employ obfuscation. All I could think of throughout this entire section was, "No. One. Cares."

And then the book ends. If you're looking for a practical book, or even an interesting book, perhaps look elsewhere. If you want to deeply ponder the ethics of privacy, well, here you go.

Lode Goukens says

read my review
http://www.civismundi.nl/index.php?p=...

Heath L LAwson says

Required Reading

I found this to be an excellent dive into the world of privacy. I paused for reflection numerous times in this book to evaluate the world around me.

BCS says

Obfuscation is the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection.

The underlying driver for considering the deployment of obfuscation techniques is due to asymmetrical relationships, characterized by an imbalance in power in a relationship, especially one in which a weaker force seeks to redress the balance in the relationship with the adversary.

Now you know this, you can start reading...

This short but powerful little book of 100 pages is presented in two sections. It begins with a ‘two-chapter’ section on the vocabulary of obfuscation, and cites many interesting cases of the application of obfuscation techniques such as using chaff to defeat military radar, or filling a channel with noise using twitter bots, through to using excessive documentation to make analysis inefficient.

The second chapter provides many thought provoking and varied examples, including, for example, using software add-ons to click all the advertisements on a web page or swapping loyalty cards to interfere with the analysis of shopping patterns.

The second section helps us to understand obfuscation, consider why it is necessary, if indeed it is justified, and whether it will work. In considering whether obfuscation will work, you need to define your project, and if you want to use obfuscation techniques, you will need to decide which of the six goals below are appropriate:

to buy some time
to provide cover
for deniability
to prevent individual exposure
to interfere with profiling
to express protest
Other questions to consider in your project definition are: is it to be carried out by an individual or does it require collective action; does it matter if your adversary knows or not; is it designed to be directed at a specific adversary (selective) or at a anyone who might be gathering and making use of data about you (general); and finally will it be over a short-term or long-term time-span?

The sheer volume of research that has been required to produce this editorial is well evidenced in the chapter notes towards the end of the book, supplemented by a further bibliography. As you would expect the text is extremely well indexed.

In summary, an enjoyable read, probably best read in two sessions - one section per session.

Review by George Williams MBCS CITP
Originally posted http://www.bcs.org/content/conWebDoc/...

Kaila says

I really wanted to love this book, but I didn't.

Pros:
1 - The beginning pages are a great compendium of different types of obfuscation and how it could relate to protecting privacy. I enjoyed that part.

2 - It's also apparent that the authors really know their stuff and have dedicated a considerable amount of time and energy into doing the research on obfuscation and then relating that to privacy.

Cons:
1 - The title is "Obfuscation: A User's Guide for Privacy and Protest", but it's not a friendly User's Guide so much as academic discourse on obfuscation and privacy.

2 - Most of Part II is written like an academic paper and is not a compelling read. Here's an example, "We beg our readers' forbearance as we sample from a vast disciplinary tradition for insights that will help us address the standoff we have identified between target and obfuscator in all its particularities."

Zzz.

3 - The font. It's small, heavy, and a sans-serif, which doesn't visually flow well.

Overall, I really like the idea behind the book, but the execution doesn't really live up to the title.

Boyan says

The book a collection of starting points for understanding and making use of obfuscation.
It is split into two parts - an analysis of the possible applications of obfuscation and obfuscation as a strategy for privacy protection; the ethical issues obfuscation raises and salient questions to ask of any obfuscation project. The authors took care to emphasize that in addition to privacy, it is not a replacement for one or all of the tools which we already rely on.
There is no simple solution to the problem of privacy, because privacy itself is a solution to societal challenges that are in constant movement.

Evan says

Like Kinney's "Hood," "Obfuscation" pairs a fantastic archive with disappointing analysis. The book starts, somewhat unconventionally, by front loading a great and extensive collection of case studies, largely, but not exclusively, drawn from the world of online big data. A certain orb-weaving spider as well as a fascinating initiative involving biometric-fooling face masks also make appearances. But it's mostly about online obfuscation.

So by the time we get to Part 2, the theoretical framework, we have a great set of data begging for analysis. So far, so good.

Unfortunately, here's where the book falls flat. A long, but surprisingly under-theorized section on the politics of obfuscation is preceded by an equally long, but even more worthless section on ethics. Seriously, STEM folk, please take a little more care to actually learn something about the philosophical traditions of ethics before purporting to apply them. A passing genuflect to Kant really doesn't cut it.

After that, the book fizzles out with a mostly redundant taxonomy of the different goals obfuscation projects might have. The space would have been much better spent trying to reach a clearer description, taxonomy and perhaps theory (hey, a boy can dream) of the techniques themselves.

Another book on surveillance culture that's more valuable for the inspiration than the actual execution.

Alex says

Fairly scattershot and overwrought. The chapter on ethics (unfortunately the longest) felt very out of place and was not greatly informative, contributing to the book as a whole feeling more like an academic essay rather than a "guide" to anything. The most interesting thing I got out of it was some insight into generalized "classes" of obfuscation or contamination that might be present in a dataset that one is analyzing, allowing one to compensate for them the analysis, though this idea wasn't explicated in the text. A fairly quick read, but I think I could have done without nevertheless.

Dana D. says

Part I is interesting enough, but less than 40 pages.

Don't waste your time with Part II. It's a repetitive lot of navel gazing reminiscent of a term paper.

Cybercrone says

This book is so NOT what the title proclaims it to be.

There is no user's guide here, just yadda-yadda that comes off like a prosecutor's opening speech (what we intend to prove here . . .) or a school paper of the BBB variety.

There is virtually nothing useful to the "user", in the sense of how-to, or even much concrete in the why-to or what-to.

I really wanted a how-to, since privacy has become so difficult to maintain, even minimally, unless you can go off-grid. And with some advocates claiming that with the use of a British company, the political parties can gather enough data to craft personalised approaches to individuals for their campaigning, it's getting downright scary.

But this book was no help.
