How to Win (at Least) Time in the Information Power Game

Author : Herbert Burkert

Date : June 3, 2016

Finn Brunton & Helen Nissenbaum, Obfuscation: A User's Guide for Privacy and Protest (MIT Press 2015).

This book is about using data noise to make your personal information less easily digestible by privacy-consuming systems.

This book is a necessary book because it presents hopeful tactics and strategies for privacy defense at a time when—in spite of half a century of debates about (electronic) privacy laws, regulations and court decisions, best practices and privacy enhancing technologies—we seem to be living in a state of privacy resignation.

This book is concise, rich with examples, written in clear language, does not shy away from the moral hazards and practical limitation of data noise creation, and clarifies again and again that privacy is about informational power relationships in which the powerless have to enlarge their options.

In the authors' words, "[o]bfuscation is the deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection" (P. 1.) clarifying that obfuscation is not about total disappearance or erasure. It is what they call a "relative utility," (P. 58.) but it is useful nevertheless. It helps to win time for privacy in the rush for completing personal profiles by the informational powerful. At a minimum, it raises the costs of gaining meaningful information and may do so significantly. The authors provide examples, historical ones, like chaff confusing anti-aircraft measures, to bring across the concept, and contemporary ones from the networked life like Twitter bots, CacheCloak, and TrackMeNot to encourage use and further design.

Obfuscation is a tool to be used when and where opting out is not an option, and where one is faced with an asymmetrical information power relationship, when it is unclear what is being done with the information with which consequences, and when there is neither trust nor adequate safeguards. "We aim," the authors say at P. 44, "to persuade readers that for some privacy problems obfuscation is a plausible solution, and that for some it is the best solution."

Yet, obfuscation poses its own moral challenges: What about dishonesty, what about wasting bandwidth, polluting or even damaging systems, what about free riding? Brunton and Nissenbaum lead us through exemplary uses of obfuscation, explaining where they see sufficient proportionality in the balance between ends and means to justify obfuscation, emphasizing that the values we attach to means and ends are ultimately social ones and as such need to be negotiated politically. For those reflecting on the use of obfuscation, the authors provide a checklist with a taxonomy of goals, threats, and benefits to allow for a realistic assessment of obfuscation's ramifications and likely success. Success, the authors hope, would not only encompass a specific outcome of a specific use of obfuscation, but widespread use that eventually leads to progress in research, regulations and policies, and to changing social practices.

Ultimately, as you are putting down the book, you become aware that with obfuscation you cannot tilt any power balance significantly. You may also wonder if these complex means of obfuscation will not accentuate that imbalance between the less and more powerful that the book's authors seek to address. But obfuscation practices may indeed catch the imagination of more system designers, programmers, and even politicians to develop structural mechanisms to counterbalance the current organizational omnipotence fantasies of foreseeability.

In the meantime it may at least help users to gain and maintain—what has been emphasized in another recently published How-to-Guide, Spy Secrets that Can Save your Life. A Former CIA Officer Reveals Safety and Survival Techniques to Keep You and Your Family Protected, by Jason Hanson—"Situational Awareness." But this was in a different context, and besides that would be a different jot …

Cite as: Herbert Burkert, *How to Win (at Least) Time in the Information Power Game*, JOTWELL (June 3, 2016) (reviewing **Finn Brunton & Helen Nissenbaum, Obfuscation: A User's Guide for Privacy and Protest** (MIT Press 2015)), http://cyber.jotwell.com/how-to-win-at-least-time-in-the-information-power-game/.