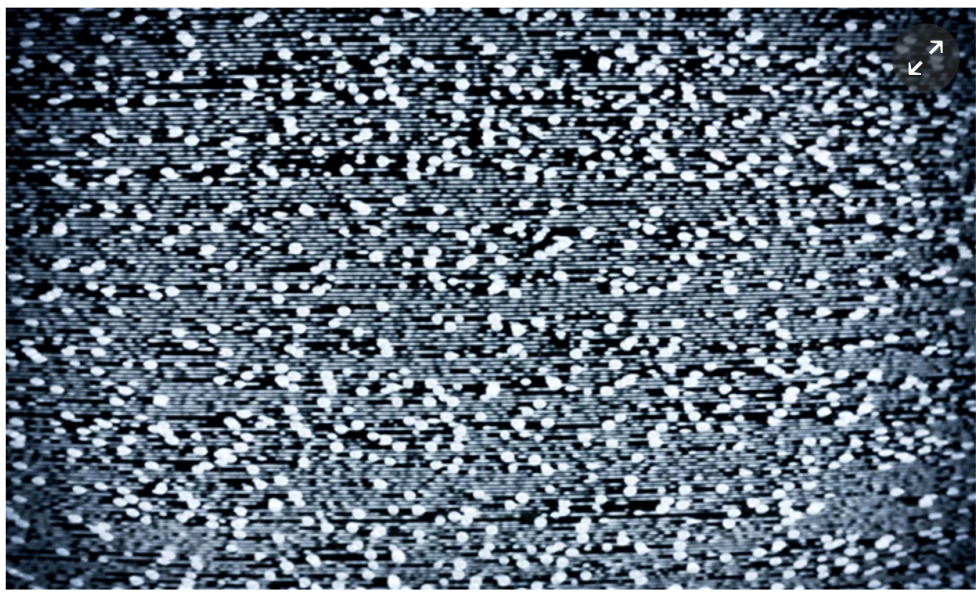
Data protection

Obfuscation: how leaving a trail of confusion can beat online surveillance

The art of obfuscation has a grand history, from 'I'm Spartacus!' to ghost radar in WWII. Could the same blurred approach give us more freedom online?

Julia Powles

Saturday 24 October 2015
09.00 BST



Obfuscation, say Brunton and Nissenbaum, is the 'addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects' to ' buy time, gain cover, and hide in a crowd of signals'. Photograph: Jon Helgason/Alamy

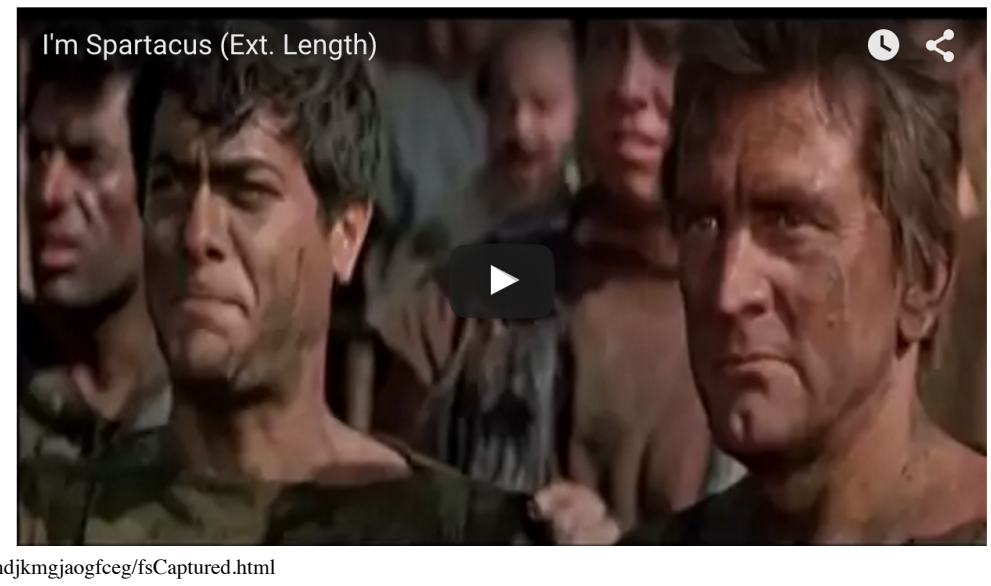
At the heart of Cambridge University, there's a library tower filled with 200,000 forgotten books. Rumoured by generations of students to hold the campus collection of porn, Sir Gilbert Scott's tower is, in fact, filled with pocket books. Guides, manuals, tales and pamphlets for everyday life, deemed insufficiently scholarly for the ordinary collection, they stand preserved as an extraordinary relic of past preoccupations.

One new guide in the handbook tradition - and one that is decidedly on point for 2015 - is the slim, black, cloth-bound volume, Obfuscation: A User's Guide for Privacy and Protest, published by MIT Press. A collaboration between technologist Finn Brunton and philosopher Helen Nissenbaum, both of New York University, Obfuscation packs utility, charm and conviction into its tightly-composed 100-page core. This is a thin book, but its ambition is vast.

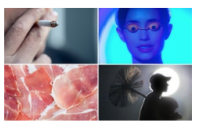
Brunton and Nissenbaum aim to start a "big little revolution" in the data-mining and surveillance business, by "throwing some sand in the gears, kicking up dust and making some noise". Specifically, the authors champion the titular term, *obfuscation*, or "the addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection projects". The objective of such measures is to thwart profiling, "to buy time, gain cover, and hide in a crowd of signals".

From poker to CacheCloak

More than 30 colourful examples - instructive vignettes in their own right - are used to build the case. Roughly a third are analogue, and the images stick. War-era choppers generating radar chaff. False tells in poker. Iconic movie scenes, like the switching briefcases in The Thomas Crown Affair, or the powerful "I am Spartacus" moment in Kubrick's 1960 epic. The authors bring in orb-making spiders, sim-card shuffles, loyalty-card swap meets, "babble tapes" (a digital file played in the background of a conversation in order to obscure it) - all examples where the individual merges with the tribe; where false signals muddy the genuine; where noise and quick feet offer "weapons of the weak".



Most popular


The 116 things that can give you cancer - the full list


South China Sea: Beijing 'not frightened to fight a war' after US move


Whale-watching boat tragedy caused by freak wave, say investigators


Which is the world's most segregated city?


Stoke turn screw on José Mourinho with shootout victory over Chelsea

'I'm Spartacus!' – obfuscation on film

Shifting to digital, noise can be destructive or productive, and it can scale dramatically. This is the landscape that a 21st-century handbook must confront. Platforms and channels can be swamped by code that mimics and distorts human communication - bots, like-farmers, decoys and hydras. Other tools, like the anonymous Tor browser, the Guardian's SecureDrop, or stylometric obfuscation (to disguise authorship), can be mission-critical for dissidents. And there is an ever growing demand for consumer-focused privacy-preserving apps, like CacheCloak, which hides your mobile location in a spaghetti map of plausible trails, or FaceCloak, which gives a layer of control over personal data within Facebook.

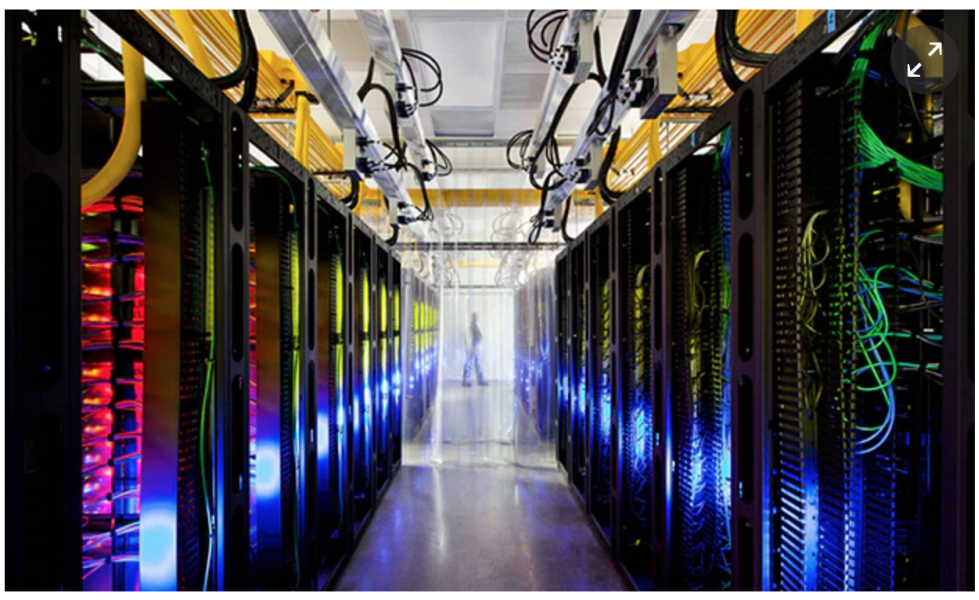
> We are naked, exposed and eminently traceable, now and into the future, by an increasing range of data-hungry agents

Most of us, most of the time, use immensely popular technologies without masks or noise. We post in what you might call corruptible silence. On Facebook, Instagram, Twitter and Google, we document our personal spaces, our frailties, our desires, questions and answers. We are naked, exposed and eminently traceable, now and into the future, by an ever-increasing range of data-hungry agents. To concerned citizens living this reality, and to thoughtful designers of technology, what Brunton and Nissenbaum offer is a compelling moral defence and some ready-to-hand tools for a small, distributed revolution of resistance.

Stunt tech, silence and saviours

Core to the book's perspective is the authors' experience in building practical tech - what they describe as "tools among other tools for the construction and defence of privacy". Nissenbaum has been the steward of two major projects, both with programmer Daniel C Howe: TrackMeNot, a search-history obfuscator that spontaneously generates clouds of possible queries; and AdNauseam, which "clicks all the ads, so you don't have to".

TrackMeNot was developed in 2006, in conjunction with developer Vincent Toubiana, while AdNauseam is new, and currently operates in conjunction with AdBlock Plus, running in the background to click every ad on a given page. Discussing the latter platform in Berlin, team-member and designer Mushon Zer-Aviv described it as, presently, more art project than mass-rollout tech. AdNauseam is currently in public beta in Firefox, but the team is working hard to bring it to Google Chrome. As Zer-Aviv described, with a hint of daring, Google will either take it down, to save ad revenue, which would be a great stunt; or it won't take it down, which would also be great.



One of Google's data centres, part of the web's back-end. Photograph: KeystoneUSA-ZUMA / Rex Features

"We see these obfuscating apps and systems as moves in a bigger picture," says Nissenbaum. "None, we think, will offer what we really need, which is comprehensive attention to the picture. Not only the big fuss about government but all the large data collectors. But they allow people to visibly signal their disgruntlement - for privacy and protest."

So how does obfuscation play into the current ad-blocking wars? "It is a devilish move by ad networks to conflate the massive back-end of tracking, aggregation, mining and profiling with advertising itself," says Nissenbaum. "Our effort, both with TrackMeNot and AdNauseam, has been targeted at the former. I don't love advertising but I can tolerate it. When supporters of the current structures of behavioural advertising say this will be the end of all the innovation and free stuff on the web, our response is: no. Although this might happen if advertising itself goes away, it does not require the back-end tracking for survival."

The worrying back-end of the web

> Advertising does not require back-end tracking for survival. **Helen Nissenbaum**

Nissenbaum is right to separate advertising and its current digital back-end. In the case of newspapers, for example, a great Faustian pact has operated between ads and content for some 300 years. It more or less works, as long as there's not too much of one or the other. The fact that this bargain is threatened by overreaching data collection and surveillance, from search engines to content-providers to third-party leeches to governments, is a measure of the urgency of our contemporary challenge and the necessity for a creative response. Obfuscation is part of that response.

There is something compelling in being persuaded of the ethical imperative of digital troublemaking by a couple of righteous academics. Obfuscation is not an academic tome, and it doesn't delve into conceptual analyses on its core principles, such as anonymity in crowds following David Chaum, or linkability following Andreas Pfitzmann. But the book has been justifiably selective to capture broad appeal. The lucid, authoritative, accessible and thought-provoking text that results is a pleasure to read.

Obfuscation is ultimately a tiny shop in the digital realm. To that extent, it has nothing against the might of big tech. But what it does have is the potential to fight to keep the preserve of human agency and autonomy uniquely human. The big hope is that when our bot descendants find this handbook stuffed in a tower in 100 years, it is unchecked surveillance - not digital disobedience - that seems antiquated.

Guardian readers on privacy: 'we trust government over corporations'

More features Topics Data protection Internet Privacy Protest Ad blocking More...