



Too much information

## Description

Someone (perhaps Slavoj Žižek) said that Trump's greatest offence is not that he breaks the law, but that he breaks unwritten norms and conventions. There's no law that says you have to be polite to everyone, say kind things, always be truthful, apologise when you make a mistake, or give credit where it's due.

Stick to the law, or weasel out of it. But to break with non-codified convention requires no such effort or defence. We think Trump does both. He breaks the law and breaks with polite convention. But let's simplify the tactic.

It is possible to obscure your actions and intentions by sticking to the letter of the law, to comply with formal requests, to do what you are told, and to deliver truthful information – and you can confound your antagonist by doing so. That's one of Finn Brunton and Helen Nissenbaum's tactics in their interesting book *Obfuscation: A User's Guide for Privacy and Protest*.

## On being unhelpful

I think anyone who works in a large organisation knows how compliance can obfuscate, particularly in relation to information: provide even more information than is asked for; provide it unfiltered and unsorted; inundate your antagonist with –paperwork– and keep it coming; exploit the fact that the requester may not really know, or forgets, what they are looking for or why they requested it.

After all, you were only asked for the information, not to be helpful. Obey the order as stated, but not un-codified good practice. (Smart managers are of course wise to this and have their own tactics and counter measures.)

## Loopholes

Here's a variant of this obfuscatory tactic. Brunton and Nissenbaum point to the use of vague language in a promise. It looks as though you are saying what people want you to say, but you say it in such a way that it provides you with a loophole in case you can't deliver on your promise: –I

promise to negotiate a deal that will deliver the best outcome.â?• Is the promise to negotiate a deal, to deliver the best outcome, or both, and the best outcome for whom?

Thatâ??s my example. They provide the example of a web service that asserts

â??Certain information may be passively collected to connect use of this site with information about the use of other sites provided by third partiesâ?• (Kindle Locations 665-669).

That looks to be showing responsibility and care for user privacy, in that the web site is telling you something. But itâ??s confusing. What we would like to read is: â??We do not collect user data,â?• but they probably do â?| and they donâ??t say that they donâ??t.



## Spreading it about

I particularly like Brunton and Nissenbaumâ??s advice on spreading culpability to protect the guilty. So activists in a group wear the same clothes as each other, including face masks, then itâ??s harder for witnesses to identify the individual who actually threw the eggs at the politician, smashed the plate glass door, or spray painted the shop window.

An obvious variant is for the individual activist to appear indistinguishable from the innocent crowd. In fact certain acts are best committed where there are crowds. If you are going to do something against the law then look the same as everyone else. The â??[I am Spartacus](#)â?• tactic is a variant. Only one person is guilty, but every member of the group or the extended group of sympathisers confesses to the crime. Outside of despotic Roman â??justice,â?• they canâ??t all technically be guilty, or punished.

The books is ostensibly about how individuals and activists can evade and subvert the way commercial interests and governments collect data about them. But the tactics are also deployed by bad actors, and obfuscation can be automated, a challenge for my next post.

## Reference

- Brunton, Finn, and Helen Nissenbaum. 2015. *Obfuscation: A Userâ??s Guide for Privacy and Protest*. Cambridge, MA: MIT Press

## Category

1. Architecture

## Tags

1. activism
2. information
3. obfuscation

## Date Created

August 24, 2019

## Author

rcoyne99

*default watermark*