

Obfuscation and its remedies

Description

default watermark

He â??took every step that he could to try to *obfuscate*, to try to get people to lie, tried to reward those people who refused to cooperate with a legitimate investigation, tried to punish and denigrate the people who were cooperativeâ•Ž (*The Hill*). Thatâ??s how the former Watergate special prosecutor (Richard Ben-Veniste) summarised the Mueller Report on Trump. I searched for â??obfuscationâ•Ž in the Mueller Report and itâ??s not there, but itâ??s all about *obstruction*.

Finn Brunton and Helen Nissenbaumâ??s book on *Obfuscation* was published before Trump was elected, and before we knew about â??Active Measures,â•Ž the operations of the Russian Internet Research Agency and of the GRU (General Staff of the Armed Forces of the Russian Federation) and their tactics to confuse, obstruct and obfuscate.

Brunton and Nissenbaumâ??s book addresses different sides of the operation: the tactics deployed by the powerful predators who want to exploit us and make money or extract political advantage from our personal information; and those ordinary citizens and (apparently) good faith activists who want to confound the attempts by powerful corporations, organisations and states to monitor, surveil, profile and coerce us.

Multiplication

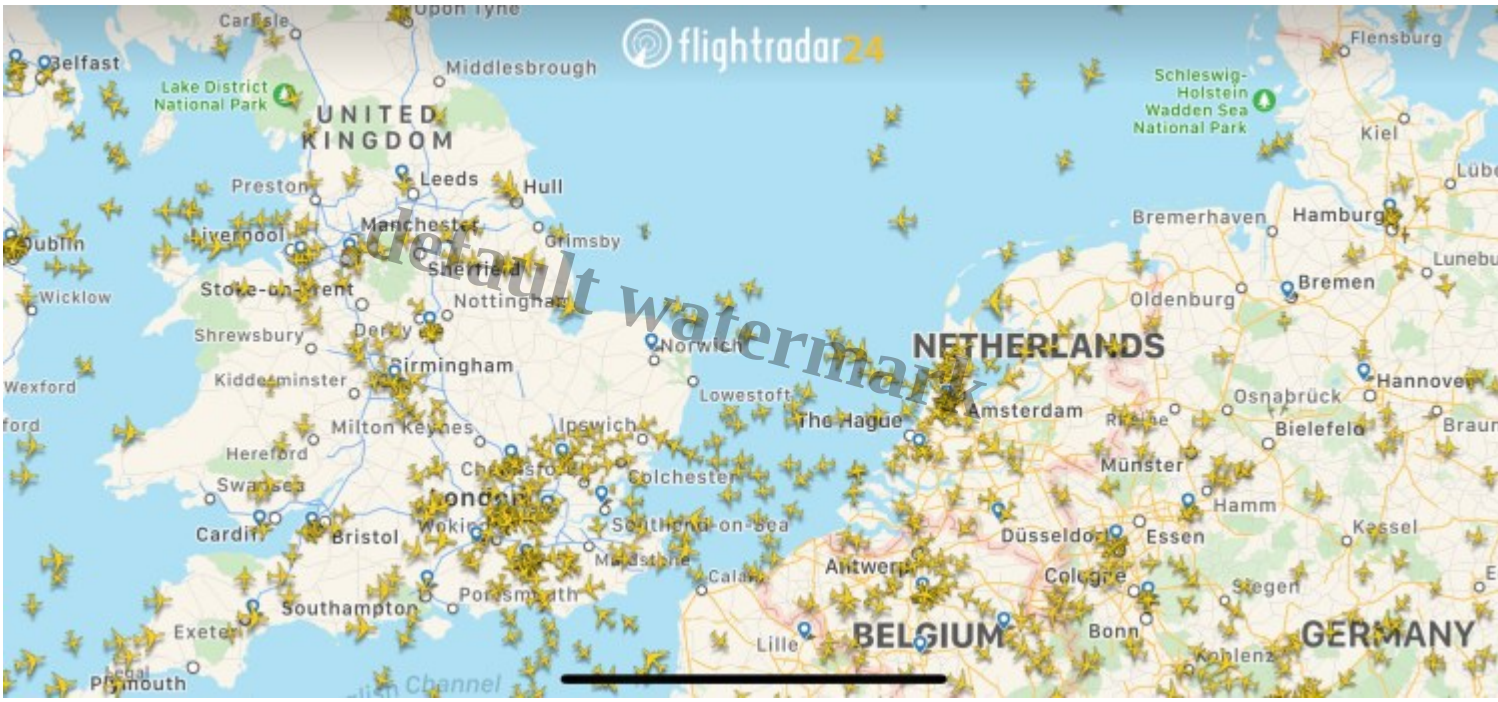
Obfuscation can be automated, or at least technologized. Brunton and Nissenbaum start with *chaff*: a technique to confound radar by scattering scraps of foil backed paper in the air. Thatâ??s a simple, low tech method to scramble radar signals to make it more difficult for the enemy to detect the location of your attack plane as it approaches its target. Thatâ??s not to hide the aircraft, but to make it look like there are more planes than there really are.

Thatâ??s the trick of obfuscation: not to hide, but to multiply, and thereby overwhelm the system of detection. Technologies are good at multiplying and repeating. Eventually the recipient of the obfuscation tactic gets the data they seek, but it takes time, even for detection tech. Obfuscation serves to delay rather than prevent detection.

Thereâ??s a mouse versus cat, prey versus predator, contest in play, as each vies against the other with ever more sophisticated means of evasion and capture. Itâ??s pretty basic, with the contest played out over various scales of organic evolution or technological development.

Brunton and Nissenbaum provide many examples of obfuscation by both good and bad actors, the powerful and the less powerful, the corporatised and the independent, the seller and the consumer, the saboteurs and the victim.

I donâ??t have a picture of an obfuscated radar display, but hereâ??s an image from the FlightRadar24 smartphone app for consumers to track the progress of commercial flights.



Bots

Twitter bots provide a conspicuous example of obfuscation by digital means. Fake twitter accounts generate new tweets, re-tweet the tweets of others, select from catalogues of standard tweets, generate likes, and generate new fake accounts to compound and confuse social media messaging.

Such tactics attempt to skew peopleâ??s impressions towards a particular point of view, to exaggerate the apparent support for one opinion or person, or simply to confuse the audience. The Mueller report makes clear that bad actors seek both to conceal (obfuscate) their own operations and to obscure the public discussion by generating fake support for conflicting opinions. The enemy seeks to divide and sow chaos.

De-profiling

On the consumer side, there are smartphone apps for confusing location data. Advertisers and profilers want to know where you are. The app sends false navigation data to the server that is trying to surveil you. It obscures your locational coordinates.

What you search for with search engines reveals a lot about you. The browser app called TrackMeNot blends fake and actual search data to obfuscate profiling. The TrackMeNot website says

> â??It does so not by means of concealment or encryption (i.e. covering oneâ??s tracks), but instead, paradoxically, by the opposite strategy: noise and obfuscation. With TrackMeNot, actual web searches, lost in a cloud of false leads, are essentially hidden in plain view.â?•

Another app called AdNauseam confounds web platforms that profile you according to the ads you click. When installed in your browser the app automatically sends clicks to the server for every ad on a page. According to their website

> â??As the collected data gathered shows an omnivorous click-stream, user tracking, targeting and surveillance become futile.â?•

Here are some other obfuscation tricks: a low tech tactic is to share SIM cards and loyalty cards to confound profilers; you can mask confidential conversations by meeting somewhere where there are a lot of voices, or deploying technologies that achieve this.

default watermark

On the bad actor side: the use of intermediaries can confuse the flow of instructions, information and funds; unscrupulous companies can generate and cancel false orders for products to overwhelm the e-commerce sites of their rivals.

Then thereâ??s â??quote stuffingâ?• used in algorithmic high frequency trading (HFT): When bidding for funds a perpetratorâ??s algorithm can deliver false quotations to slow down their competitors. The perpetratorâ??s algorithm ignores these false bids because they made them, but their competitor canâ??t. Sifting through false information slows down your opponentâ??s bidding. Thatâ??s described in section 2.5 of Brunton and Nissenbaumâ??s book.

Cutting through the noise

Brunton and Nissenbaum write about obfuscation as a delaying tactic, which simply gives time for the the prey to escape, or the attacker to break the defences. Obfuscation is not fail proof. To put a pile of papers on the bossâ??s desk may obfuscate the one piece of information that sheâ??s looking for, but if the documents are organised, like a book, with a table of contents and an index, then the vital information is easier to find. The obfuscator is unlikely to provide an index however. Were they to provide a set of digital text files they could be searched or even processed with sophisticated software that looks for patterns.

When the US Department of Justice first made the Mueller Report available to journalists and the public it was released as an image file. Every page was a digital optical scan, but you couldnâ??t search that for words or phrases. I think that was an initial means of obfuscation. I tried to run the file through Adobeâ??s optical character recognition (OCR) function, but the file was too big. Eventually, a week or so later, a searchable version appeared online.

Whether searching a single document or the entire Internet, search algorithms donâ??t check each word of the document in sequence in real time till they hit the target. That would be too slow. The software creates an index, in the background as it were, when nothing else is happening. Itâ??s smart indexing that makes Internet searches so fast. As with encryption and decryption methods, the

escalation of tech developments makes both tactics for obfuscation and breaking through the noise more difficult.



default watermark

Bibliography

- Brunton, Finn, and Helen Nissenbaum. 2011. Vernacular resistance to data collection and analysis: A political theory of obfuscation. *First Monday*, (16) 5, https://firstmonday.org/article/view/3493/2955.
- Brunton, Finn, and Helen Nissenbaum. 2015. *Obfuscation: A Userâ??s Guide for Privacy and Protest*. Cambridge, MA: MIT Press
- Manchester, Julia. 2019. Mueller report suggests Trump intended to obstruct investigation, says ex-Watergate prosecutor. *The Hill*, HILL.TV. Available online: https://thehill.com/hilltv/rising/440192-evidence-in-mueller-report-suggests-trump-had-intent-to-obstruct-probe-says-ex (accessed 8 August 2019).
- McIntyre, Lee. 2018. *Post-Truth*. Cambridge, MA: MIT Press
- Mueller, Robert. 2019. *Report on the Investigation into Russian Interference in the 2016 Presidential Election*. Washington, DC: US Department of Justice

Note

- Multiplication and delay are two recurrent themes in obfuscation. Hereâ??s another trumpian tactic. Following yet another mass shooting, the audience would like to hear Trump condemn white nationalism. Instead, he multiplies the guilty parties: â??I am concerned about the rise of any group of hate â?¦ whether itâ??s white supremacy, whether itâ??s any other kind of supremacy â?¦ whether itâ??s Antifa, whether itâ??s any group of hate â?¦ I am very concerned about it and Iâ??ll do something about it.â?• Iâ??m quoting from a video posted in the Guardian on 7 August 2019. The delay part comes with trying to unpack this. By the time you realise the only group heâ??s identified by name is an activist group that is in fact opposed to white nationalism, the questioning has moved on â?¦ as has the so-called news cycle. It takes time to detect that an issue has been *obfuscated*. One of the antidotes is the justly-acquired scepticism about anything Trump ever says â?? a rational pre-judgement, a healthy bias against known

perpetrators of untruths and obfuscations. See posts on hermeneutics.

Category

1. Economics

Tags

1. Mueller Report
2. obfuscation
3. surveillance
4. trump

Date Created
August 31, 2019
Author
rcoyne99

default watermark