Is it possible to fool an algorithm? Making a case for data obfuscation

By Fieke Jansen & Maya Indira Ganesh
Tactical Technology Collective
https://tacticaltech.org

A proposal for preliminary work to document how data obfuscation as a privacy enhancing strategy works in distorting the algorithmic profiling of users.

Information asymmetries in big data environments

The data industry is huge, growing and opaque. The industry is comprised of companies that work as data suppliers, data management platforms, data exchanges, sales houses, advertising networks, demand side platforms and various other commercial agencies[1]. These companies collect, process, aggregate, label and sell user data. This has created an information asymmetry between such companies and individual users I.e data holders/suppliers; users cannot see, control or interpret the data that is collected about them, nor how it is used and who it is sold to.

This makes it impossible for users to challenge their data's potential misuse or misrepresentation. The lack of information about how exactly users' data is collected and aggregated makes it near impossible for advocates and activists to mount a case for regulation of any kind. Data industries operate under a “veil of secrecy”[2] and are not easy to understand and comprehend as a whole.

The decisions governing data collection processes occur beyond user control. These decisions, in part, algorithmic processes, are governed by commercial privacy policies, data protection regulation and self-regulation. In reality these processes are limited and are not addressing systemic issues of user privacy and data security.

Data and technology are intrinsic parts of people's everyday lives, yet digital privacy enhancement and security skills are generally low. To empower individual users, governments and corporations suggest solutions that are based on the assumption of informed consent, a concept that is problematic at best, broken at worst. It is in this context that responsibility for data privacy and security is shifted onto the individual user. Privacy-awareness groups suggest technical solutions that range from opting out, to encryption and anonymising tools. Many of these solutions can be cumbersome, difficult to understand and manage and require a level of technical skill that is beyond the grasp of average internet users. There are some people who can and do have the requisite skills, but it is not known how and if they work against the ever-increasing quantification of the internet.

Therefore, this is a proposal for preliminary work towards auditing algorithms by creating resistance to them, namely data obfuscation tools and tactics. The question we are trying to address is if and how strategies for data obfuscation impact the algorithmic profiling of users. We propose to do this by examining the outputs of generic websites and queries through the use of different privacy enhancing strategies. This is not intended as a stress test of privacy enhancing tools.

[1] Improve Digital. Display Advertising Ecosystem 2015 http://www.improvedigital.com/en/market-map

[2] Committee on Commerce, Science & Transportation (2013) 'A review of the data broker industry: collection, use and sale of consumer data for marketing purposes' Accessed March 22, 2015 http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=0d2b3642-6221-4888-a631-08f2f255b577

Data Obfuscation

Data obfuscation is a tactic to hide sensitive data in a large dataset with 'random' noise data so that it can 'hide' in the 'crowd'. Finn Brunton and Helen Nissenbaum define data obfuscation as “an alternative strategy of informational self-defence, a method that acts as informational resistance, disobedience, protest or even covert sabotage – a form of redress in the absence of any other protection and defence, and one which disproportionately aids the weak against the strong...is the production of misleading, ambiguous and plausible but confusing information as an act of concealment or evasion[3]. While the strategies of opting out, legal protection and encryption come with challenges and reliability issues, the data obfuscation strategy has been the least researched nor tested.

Profiling algorithms employed by data brokers are only as valuable as the types, amount and accuracy of the data the algorithms can access. If there is no data to collect and aggregate, then profiling is not possible and therefore lacks value. If the data is corrupt, then the value of the profiling algorithm decreases. The question is about understanding the impact of the obfuscation strategy on the profiling algorithm. Specifically, little is known about how exactly data obfuscation works in relation to algorithms that identify and profile the user. Does it work at all, and if so, how?

Research problem & method

How does the Facebook algorithm serve news feeds differently to the activist who is using multiple tactics of data obfuscation, as compared to the activist who is less concerned about privacy and is working in the same thematic domain? ('domain' refers to issue areas and movements, like women's rights, LGBTQI rights, anti-corruption etc)

We frame this research question focusing on a community and audience that Tactical Tech works with: social justice activists. In our work we find that communities of activists who need to use the internet in their everyday lives and professional organising, mobilising and in exposing corruption and injustice face considerable risks because of the 'data shadows'[4] they leave behind. For the past 12 years we have also been engaged in digital security and privacy capacity building; many of our audiences actively use privacy enhancing techniques and tactics in their work. We are therefore interested in understanding how algorithms respond to data obfuscation tools and tactics.

In order to do this we propose comparing results and content over time for queries made by a number of people using and not using obfuscation tools and tactics. This will enable us to compare the outputs of the testers who are similar (in intent) but are using different privacy enhancing strategies (these are our variables). The aim is *not* to test the strength of privacy enhancing tools used in these strategies, but to see how the results differ. This could allow us to see how these strategies have an impact on the Facebook algorithm, almost as if we were auditing the algorithm to see how it responds to challenges to profiling. Individuals would set up a new Facebook account, befriend the same people, but not each other, like similar content and campaigns but apply different privacy strategies every time they access Facebook. After a series of such actions, the results of their news feeds could be compared. The different privacy enhancing strategy variables are:

- No strategy
- Strategy of using privacy enhancing tools - VPN
- Strategy of using privacy enhancing tools - TOR
- Strategy of using obfuscation – OpenPaths (https://openpaths.cc/)
- Strategy of using obfuscation – AdNauseum (http://dhowe.github.io/AdNauseam/)
- Strategy of using obfuscation – FloodWatch (https://floodwatch.o-c-r.org/)

[3] Brunton, F & Nissenbaum, H (2012) Political and ethical perspectives on data obfuscation in *Privacy, Due Process and the Computational Turn* (Eds.) Mireille Hildebrandt and Katje de Vries, New York: Routledge, 164-188

Accessed April 12, 2015. Nissenbaum also initiated the Ad Nauseum tool http://dhowe.github.io/AdNauseam/

[4] More on our project about informing users about taking back control of their data here, at My Shadow https://myshadow.org

Goals

Tactical Tech's goals in applying for this workshop are:

1) What can we learn about how profiling algorithms affect communities that need to mask their digital traces and identities online?
2) What happens to profiling algorithms when they are challenged through data obfuscation and privacy enhancing tools?
3) How can we start to consider what the possible strategies of resistance are to algorithmic regulation?