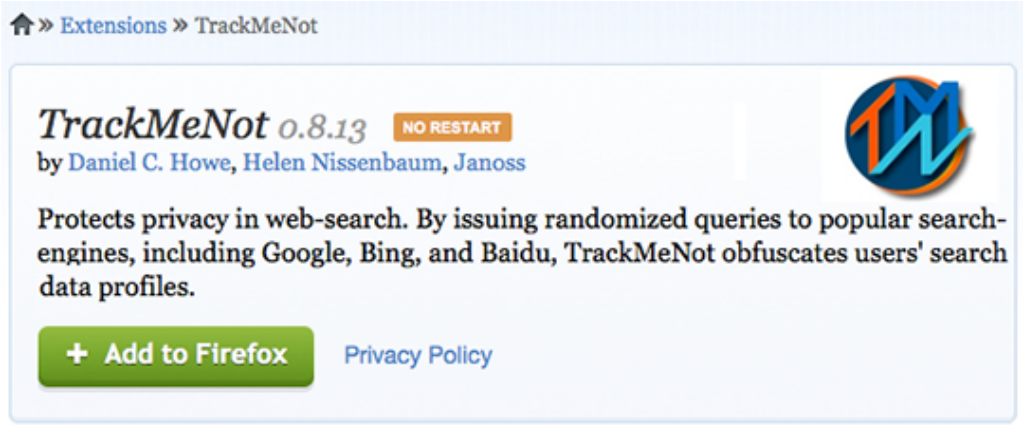
Daniel C. Howe, Ph.D., Assistant Professor, School of Creative Media, City University Hong Kong.

> [T]o radically automate and to automate radically as a careful ethical and aesthetic gesture. (Munster)

The ubiquity of the web-browser as an interface to the web, and to digital content in general, has by now surpassed that of any other software entity. Some designers have even made the case that the browser represents a key locus for the inculcation of obedience in contemporary society. On each page we are forced to learn or adhere to the rules of a different set of site designers or administrators without any say whatsoever in what those rules might be (Zer-Aviv). Whether or not one accepts such claims, the browser remains a key focal point for much of the surreptitious data gathering and surveillance that pervade the web. As researchers have shown, there are a multitude of vectors by which corrupt advertisers, repressive governments, and other malicious players can attack the browser to identify its user and access valuable personal data without consent. Due to the breadth of the attack surface that the browser provides, there is little that the average users can do to defend themselves. If you are not identified and tracked by cookies, ad-malware, tracking-code, or browser fingerprinting, then caching and timing attacks are likely to get you in the end (Janc and Zalewski). One avenue that has shown promise in frustrating data collection in the browser, however, has been obfuscation. Obfuscation, defined as "[t]he production, inclusion, addition, or communication of misleading, ambiguous, or false data in an effort to evade, distract, or confuse data gatherers or diminish the reliability (and value) of data aggregations" (Brunton and Nissenbaum), has in part proven successful as a strategy due to the ubiquity of the browser itself. While a web service provider may be able to filter out unwanted requests from individuals, it is far more difficult when tens of thousands of different users are attempting to pollute their captured data in this way. As such, obfuscation may represent a useful avenue of resistance against contemporary datafication in online space.

While obfuscation has a long history in both the analog and digital realms, its direct application to online datafication (the quantification and subsequent monetization of human activity) dates back at least to the 2006 release of the TrackMeNot browser plugin.[1] The specific problem that this project addresses is the collection and aggregation of sensitive personal data during search.

Implemented as a free plugin for Firefox and Chrome, TrackMeNot works by sending 'decoy' queries to popular search engines like Google, Bing, or Baidu, whenever a user searches, hiding their actual interests in a cloud of algorithmically-generated 'noise'. The tool is designed to increase the difficulty of aggregating such data into either accurate or identifying user profiles. AdditionallyTrackMeNot attempts to provide, "for some users a means of expression, akin to a political placard or a petition. For others it provides a practical means of resistance… to large-scale systems of surveillance". The technology is described as a form of political action, building on work by Langdon Winner and Bruno Latour, who have argued that technical devices and systems may embody political and moral qualities.



From these comments, we can see that while TrackMeNot is often grouped with other tools to protect 'privacy', there is a larger agenda at play, specifically an expressive (a term we will return to below) resistance to quantification as means of managing human experience. Munster, in her description of what is at stake in the project, says the following:

> Data mining is a technique that belongs to knowledge economies modulated by the diffuse politics of biopower… the historical shift, in western societies at least, from governing the individual to managing populations via techniques such as the statistical analysis and prediction of lifespan, habit, custom and so on (Foucault, Lazzarato). These techniques for managing populations now saturate 'life' and can be found everywhere… We cannot simply champion privacy and the individual against ubiquitous surveillance and the corporation. We need to look carefully at the technical forces at work in networks for they both modulate and generate power and potentialities.

The artist Eduardo Navas may have recognized these larger dynamics at play when he selected TrackMeNot as the source for his own work Traceblog. Over the course of this five-year project, Navas ran TrackMeNot in his primary browser continuously from April 2008 to April 2013, and reposted each of TrackMeNot's generated searches to the Traceblog blog (he does not post any of his actual searches). He writes:

> [w]hat I find most interesting about TrackMeNot is that the pseudo search results are somewhat a reflection of what I do online. According to the developers of the Firefox extension, TrackMeNot keeps track of the actual searches and with time begins to assimilate parallel results that somehow reference indirectly what the user would search for... It's like having my own double, a clone about whom I'm learning more and more about. I like this about TrackMeNot, and it was actually the first thing that interested me about it... For me Traceblog is another project in which I aim to explore the implications of the growing pervasiveness of information flow and its manipulation.

Munster, in a review of the two works, makes explicit the link between this manipulation of information flow in the service of datafication and obfuscation as a counter-strategy, suggesting that we "not simply retreat or withdraw into the issue of privacy", but rather "become noisy, as noisy as our machines" (Munster).

Not all critics were as positive as Navas and Munster however. TrackMeNot also generated significant controversy, with one blogger referring to the prototype as the "Worst Security Tool Ever" (Hilton, 2006). Some critics questioned TrackMeNot's effectiveness against machine-learning attacks, some cast it as a misuse of bandwidth, and others found it unethical. While these arguments were

discussed in some detail in a paper describing the project (Howe and Nissenbaum, 2009), it is interesting to note the degree to which the project was initially derided by the security community, though the larger strategy, often referred to as 'privacy-via-obfuscation', has developed into an active subfield of computer science research. Perhaps equally interesting are the obfuscation-based projects which may have been inspired by TrackMeNot.[2]

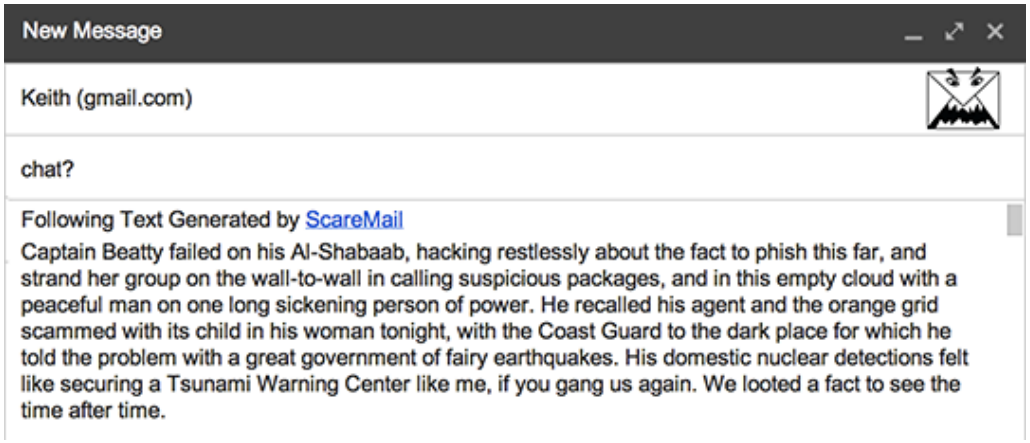
One such project, I Like What I See, by Steve Klise, is a web browser extension that automatically clicks all 'Like' links on Facebook. As with other successful works employing obfuscation as a strategy, the project can be described quite succinctly. On the project's Github page, Klise writes:

> When you visit Facebook, click the thumbs up in the extension bar and start scrolling and liking. Liking and scrolling. Every instance of the word 'Like' will be clicked. Don't worry, Facebook is a fun place full of all of the stuff you like.

Liking 'everything' serves to obfuscate your true interests, in this case, from Facebook. However it is likely to also yield second-order effects, specifically the pollution of your social media streams with all manner of strange automated content; a phenomenon described in some depth by Honan.

ScareMail by Ben Grosser is another web browser extension that employs obfuscation in the context of email surveillance. Extending Google's Gmail, ScareMail adds to every new email's signature an algorithmically-generated narrative containing NSA search terms. This narrative acts as "a trap for NSA programs like PRISM and XKeyscore, forcing them to look at nonsense". Grosser describes the project as follows:

> ScareMail proposes to disrupt the NSA's surveillance efforts by making NSA search results useless. Searching is about finding the needles in haystacks. By filling all email with 'scary' words, ScareMail thwarts NSA search algorithms by overwhelming them with too many results. If every email contains the word 'plot', or 'facility', for example, then searching for those words becomes a fruitless exercise. A search that returns everything is a search that returns nothing of use.



Closely following justifications for TrackMeNot (Howe and Nissenbaum), ScareMail proposes "a model of privacy built on visibility and noise as opposed to one built on encryption and silence" (Grosser).

AdNauseam, perhaps the most direct descendant of TrackMeNot, is a browser extension designed to obfuscate browsing data and protect users from surveillance and tracking by advertising networks. The plugin works with existing adblockers to block ads on visited pages, but then quietly clicks each ad in the background, polluting user profiles and creating mistrust between advertisers and the networks they pay for clicks. In addition to protecting users, AdNauseam attempts to amplify their discontent with advertising networks and shift the balance of power between the trackers and the tracked. One unique property of AdNauseam is its support for the notion of sousveillance,[3] via its 'AdVault' feature, which allows users to explore interactive visualizations of the ads they are served, providing an algorithmic glimpse into their profile as perceived by the advertising networks (Howe et al.).

A number of relatively recent projects have extended obfuscation strategies beyond the browser and into the terrestrial world. Facial Weaponization Suite, by Zach Blas, attempts to intervene against biometric facial recognition by making 'collective masks' in community-based workshops that are modeled from the aggregated facial data of participants. These amorphous masks are not only aesthetically interesting, but apparently cannot be detected as human faces by biometric facial recognition technologies. One such mask, the Fag Face Mask, generated from the biometric facial data of queer men's faces, challenges scientific studies that link the determination of sexual orientation with facial recognition techniques.Another mask takes up biometrics' deployment as a border security technology and the resulting violence and nationalism it instigates. These masks intersect with social movements' use of masking as a tool for collective transformation that refuses dominant forms of representation.

Invisible, by Heather Dewey Hagborg, applies obfuscation to the context of genetic privacy in the physical world, erasing and obfuscating traces of your DNA to frustrate identification. The Invisiblekit, available in a limited edition of 100 as a

retail item from the New Museum store,[4] is a suite of two complementary products. The Erase™ spray deletes 99.5% of the DNA you leave in public, while the Replace™ spray cloaks the remaining .5% with DNA noise. In a recent email exchange, Hagborg states that "the idea of an obfuscation DNA spray was actually inspired in part by Nissenbaum's talk at PRISM break up last year" (Hagborg).

While the specifics of these projects vary, there are common elements we can identify. The first is that they all critically address the trend toward datafication made possible by algorithmic processing of data at scale. Scale is important in that it necessitates the use of machines for the collection and analysis of data, and, in most cases, removes human observations from the equation. Thus it is worth reiterating the point that obfuscation technologies generally target algorithmic systems (even in apparently non-digital cases like radar chaff or loyalty card-swapping[5]). In fact, as the types of noise introduced into these collection systems can often be identified by human analysis (consider ScareMail, where a human observer would quickly be able to recognize the type of 'noise' being generated), it is specifically the machinic nature of such systems that is targeted. For this reason, obfuscation can be situated within a larger class of strategies, as described by Gary Marx, whereby individuals attempt to resist surveillance by taking advantage of the blind spots inherent in large-scale systems (Marx). Due to the scale of such systems, obfuscating technologies will generally rely on automation to achieve their ends; though this is not the instrumental automation that drives capital relentlessly onward, requiring still more automation at each subsequent step. Instead it is a tactical automation so limited in scope and context that its end goal is often to erase the need for itself. As the authors of TrackMeNot state, the goal of TrackMeNot is to, eventually, eliminate the need for TrackMeNot. Or, as Munster eloquently puts it, "to radically

automate and to automate radically as a careful ethical and aesthetic gesture.The hope remains, even if this endeavour fails, of creating a more poetic pattern aimed at disaggregating behavior as a predictive and normative construction." (Munster)

This type of tactical, even 'poetic', resistance to automation at scale suggests the categorization of obfuscation-based tools as expressive technologies. That is, they exist not only to serve some instrumental function, but always also to amplify social, cultural or political perspectives. The expression that such tools facilitate is generally of a fundamentally different type than that which the technical system condones, though on the surface they may look similar. Take the example of web-search, in which users are expected to participate in the search system in exactly one way; that is by entering terms into the search box, and then clicking 'go'. Once these data bits have been transferred across the wire to the search 'engine', no further input from the user is allowed. The vast architectures of crawling, indexing, aggregating, and filtering – leading directly to surveillance – reside on the far side of this impermeable membrane, visible only through the tiny window that the search box represents. As this search box is the one permitted avenue of input into the system, it is the search-box that obfuscatory technologies must rely upon. The constraints of the interface (and secondarily, the protocol employed) are necessarily ones that obfuscating technology must grapple with. TrackMeNot tackles such constraints directly, in effect saying, "indeed, we will use the search box you have mandated, but we will do so toward the realization of quite different ends than you intend". This re-assertion of agency in relation to both interface and protocol is a key locus through which obfuscating tools may realize their expressive power, amplifying the voices of those arguing for alternate criteria for value (privacy, autonomy, freedom, etc.) in technical systems.

Obfuscating systems also represent communal strategies, in contrast to more traditional security-oriented approaches focusing on protection of the individual. At a basic level, the tools discussed above can be understood to be communal simply to the degree that they are expressive; the amplification of non-dominant social voices can be conceived as communal practice in itself. Further, as Howe and Nissenbaum point out, some of these tools work communally in a stronger sense. The degree to which noise generated by obfuscation tools diminishes the value of the collected data in systems can serve to protect even those not using the tools. Even in cases where the removal of such noise is possible, one must consider the resources required to do so. Recent research on data mining show

that the removal of noise from data-mining systems already occupies significant resources, with upwards of 80% of project time reported as being spent on the cleaning and preparation of data.[6] Thus even small amounts of additional noise added to systems may cause significant costs to data-mining service providers, and thus influence future decisions on what information to collect and store, and even, potentially, on whose views to consider when making such decisions.

So then, to what extent do the obfuscation tools mentioned share common goals? Though varying from work to work, one superset of goals that we might identify includes protection, expression, and subversion (see figure 1). The first of these, protection, refers to the degree to which the tool attempts to protect individuals and communities from harms. We have explored the notion of expression above, referring to the degree to which the tool facilitates the amplification of user voices in the dynamic at hand. Lastly, subversion refers to the degree to which the tool attempts to undermine the larger system against which it is acting. So in the case of AdNauseam, the tool manifests three primary aims: a) to defend users against tracking by advertisers (protection); b) to provide users with a means of voicing their frustrations with the advertising system (expression); and c) to inject uncertainty into relations between ad-networks, advertisers, and websites, whose interests have, to this point, been largely aligned (subversion).

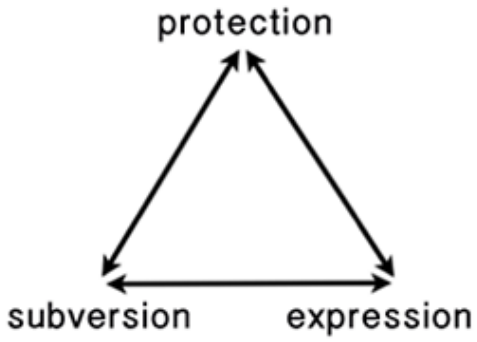


Fig. 1. Obfuscation goals

Each of these goals appears present to some degree in the systems described above, however their relative importance varies from tool to tool. In the historical case of radar chaff for example, protection (of attacking fighter planes from radar) appears tantamount, while expressive and subversive elements are relatively unimportant. For ScareMail, however, expressive and subversive elements are foregrounded, while protection is relatively unimportant; the tool does not appear

designed to actually protect users who are attempting to use NSA trigger words in their emails, but instead to express a larger critical point about surveillance, and to subvert the effectiveness of this type of bulk surveillance system.

There may also be relationships between goals that are worth exploring. For obfuscation to function as protection, the noise generated by a system must exhibit a high degree of indistinguishability with regards to the data the system intends to capture. It must generally be difficult for an adversary to distinguish this noise from the data it is attempting to collect.[7] However if we imagine a tool that is perfect on the protection dimension – one for which it is never possible to filter noise from data – then the system would be functionally invisible to the adversary. The expressive capabilities of such a perfectly invisible system, however, would likely be minimal, as the adversary is literally unaware of the injected noise.[8] Conversely, if a system is highly expressive, it may be easier for an adversary to filter the noise generated, thus diminishing the tools protective capabilities. In the case of ScareMail, for example, it would not be difficult for an engaged adversary to both detect users of the tool and to filter out the trigger-word-laden signatures generated by the system. However, in an odd twist, such filtering might also serve to create temporary spaces free of surveillance. If, for example, an adversary was filtering (and ignoring) data from the ScareMail signatures, this might create a free zone for messaging not subject to trigger-word monitoring. A similar situation might occur in the case of AdNauseam. Were an ad-network to decide to filter all clicks by users of the tool, such users would then be in the interesting position of being ignored by the advertising systems to which they are objecting.

So while there appears to be at least a somewhat inverse relationship between goals of expression and protection, there are interesting counter-examples to consider. For example, we might imagine a tool that is easily detectable, but which generates data that is highly indistinguishable. TrackMeNot itself is an example of a detectable tool, in that it is trivial for a search engine to notice the increased frequency of queries for users who install it. However this does not imply that the search engine can easily filter the noise generated by such a tool (see Gervais et al.for an analysis of this question for the case of TrackMeNot). An adversary may be aware that a tool is injecting noise into its system, yet be technically, culturally, or otherwise unable or unwilling to filter it. In such a case, we might imagine the tool to be successfully protecting the user and facilitating a high degree of expressivity. Whether such a tool does (or can) exist in practice is

another question.

To conclude, one term that may be useful in conceptualizing projects that leverage obfuscation as a means of critiquing datafication is the notion of 'data undermining' (Munster). To data undermine, according to Munster, is not only to leverage the same data and network structures responsible for datafication as a means of investigating and critiquing it, but to do so via aesthetic strategies. Such strategies, which she describes as an "aesthetico-political set of practices and directions for contemporary networked culture", relate not to how such work looks, but rather to what it allows us to see – specifically the data, algorithms, and relations that capital networks obscure. This verb, 'to obscure', from the latin fuscare ('to darken') is of course one of the roots of obfuscation (together with ob- 'over or against'), an interesting counterpoint with the aesthetic strategy of making visible. Munster says,

> The poetics of data undermining as a networked art approach lie in how extensions, aggregators and plugins use display as a mode of intervention into the spaces of existing web design. There is a poetics in the creation of networked spaces in which alternative forms of sociality might be invented and which cut across predesignated arenas for online interaction.

It is perhaps this very revealing of hidden mechanics, what Munster describes as the attempt to "poetically render perceptible the interests at stake", that makes possible the imagination of the alternative social forms suggested by the projects above.

Notes

[1] TrackMeNot (http://cs.nyu.edu/trackmenot) is a project by the author and Helen Nissenbaum. Earlier examples do appear in the literature, especially for location-based privacy (see Duckham and Kulik), however such systems generally focused on the restriction of information released, rather than on the addition of noise.

[2] Several such projects have been described by Brunton and Nissenbaum, including FaceCloak (Luo, et al.), BitTorrent Hydra (Schulze and Mochalski), and CacheCloak (Meyerowitz and Choudhury). There have also been a number of subsequent obfuscation schemes for the search case, five of which are detailed,

and compared to TrackMeNot in Balsa et al.

[3] 'Sousveillance' is a term coined by wearable-computing pioneer Steve Mann to describe inverse surveillance. The term comes from the French 'sous' (from below) and 'viller' (to watch); to watch from below. Mann suggests that societies may employ sousveillance "as a way to balance the increasing (and increasingly one-sided) surveillance".

[4] See http://www.newmuseumstore.org/browse.cfm/invisible/4,6471.html

[5] Radar chaff and loyalty card-swapping are two cases of early obfuscation strategies described in Brunton and Nissenbaum.

[6] One data analyst states "going back to the key question of this article: what fraction of time is spent in data preparation for modeling?... I have continued to ask this question of any group of analysts I happen to meet, and the answers have been remarkably consistent: the most common response is 80%. Literally hundreds of practicing data miners and statistical modelers, most of them working at major corporations supporting extensive analytical projects, have reported that they spend 80% of their effort in manipulating the data so that they can analyze it" (Steinberg).

[7] Computer science researchers have advanced interesting definitions of how this difficulty can be measured. See Balsa et al. and Gervais et al. for two such approaches (both of which include TrackMeNot in their analysis.)

[8] One additional question might involve the specifics of the definition of 'expressivity' being applied. In the case above we appear to require an adversary to be aware of a system for it be considered expressive. Yet this does seem a necessary component of the definition. One can, for example, imagine a system that has no measurable effect on an adversary, but still allows users to feel that they are acting expressively nonetheless. The adversary simply does not hear the user's expressive voice. Whether such expression is 'real', much like the question of whether a painting that no one views can still be considered art, is beyond our scope, however it is interesting to note that such a system might be considered ideal from the perspective of the adversary; a system that appears to afford users with greater voice, but actually has little real-world effect. Examples here might include the case of online petitions, or the current DoNotTrack standard, both of which likely have little instrumental effect, but may create a sense of expression in the user. In a pessimistic analysis, such potentially 'inauthentic' expression

could work to diminish the likelihood of individuals taking other, possibly more effective, actions.

Works cited

Balsa, Ero, Troncoso, Carmela, and Diaz, Claudia, 2012. “OB-PWS: Obfuscation-Based Private Web Search”. Proceedings of the 2012 IEEE Symposium on Security and Privacy (SP ’12). IEEE Computer Society, Washington, DC, USA. 491-505. Print

Blas, Zach, “Facial Weaponization Suite”, n.p. 2011. Web <http://www.zachblas.info/projects/facial-weaponization-suite>.

Brunton, Finn, and Nissenbaum, Helen. “Vernacular resistance to data collection and analysis: A political philosophy of obfuscation,” First Monday, 16.5 (May 2011). Web <http://firstmonday.org/article/view/3493/2955>

Duckham, Matt and Kulik, Lars. “A formal model of obfuscation and negotiation for location privacy”. Proceedings of the Third international conference on Pervasive Computing (PERVASIVE’05). Eds. Hans-W. Gellersen, Roy Want, and Albrecht Schmidt. Berlin, Heidelberg: Springer-Verlag, 2005. 152-170. Print.

Drucker, Johanna. “Humanities Approaches to Graphical Display.”Digital Humanities Quarterly 5.001 (2011). Web <http://www.digitalhumanities.org/dhq/vol/5/1/000091/000091.html>

Gervais, Arthur, Shokri, Reza, Singla, Adish, Capkun, Srdjan and Lenders, Vincent. “Quantifying Web-Search Privacy.” Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS ’14). New York, NY: ACM, 2014. 966-977. Print.

Grosser, Ben. “ScareMail.” 2013. Web <http://bengrosser.com/projects/scaremail/>.

Hagborg, Heather D. “Re: [artsec] Looking for a collaborator.” E-mail to [Author], 21 Nov. 2014.

Hilton, Rod. “Worst Security Tool Ever”, Blog: Absolutely No Machete Juggling. Aug 2006. Web <https://web.archive.org/web/20061028105420/><http://blog.air0day.com/2006/08/21/worst-security-tool-ever/>.

Honan, Matt. “I Liked Everything I Saw on Facebook for Two Days. Here’s What It Did to Me”. Wired.com 14 Aug. 2009. Web <http://www.wired.com/2014/08/i-liked-everything-i-saw-on-facebook-for-two-days-heres-what-it-did-to-me/>

Howe, Daniel C. and Nissenbaum, Helen. “TrackMeNot: Resisting Surveillance in Web Search.” Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society. Eds. Ian Kerr, Carole Lucock and Valerie Steeves. Oxford: Oxford University Press, 2009. 417-436. Print.

Howe, Daniel C. “Obfuscation and its Discontents: DIY Privacy from Card Swap to Browser Hack”, at HopeX, New York, NY. July 18, 2014. Print.

Howe, Daniel C. and Nissenbaum, Helen. “TrackMeNot.” New York University Computer Science Aug. 2006. Software/browser extension <http://cs.nyu.edu/trackmenot/>

Howe, Daniel C., Nissenbaum, Helen, and Zer-Aviv, Mushon. “AdNauseam.” n.p. 2014, Software/browser extension <http://dhowe.github.io/AdNauseam/>

Janc, Artur and Zalewski, Michal. “Technical analysis of client identification mechanisms.” The Chromium Projects, 2014, Web. 28 Nov, 2014. <http://www.chromium.org/Home/chromium-security/client-identification-mechanisms>

Klise, Steve. “I Like What I See.” 2012-14. Software/browser extension <https://github.com/sklise/i-like-what-i-see>.

Luo, Wanying, Xie, Qi and Hengartner, Urs. “FaceCloak: An architecture for user privacy on social networking sites.” Proceedings PASSAT ’09: 2009 IEEE International Conference on Privacy, Security, Risk and Trust (Vancouver, B.C.). 26–33. Print.

Mann, Steve. “Sousveillance: inverse surveillance in multimedia imaging,”. Proceedings of the 12th annual ACM international conference on Multimedia. New York, NY: ACM, 2004. Print.

Marx, Gary T. “A Tack in the Shoe: Neutralizing and Resisting the New Surveillance,” Journal of Social Issues, Vol 59, No. 2, 2003: 369-390. Print.

Meyerowitz, Joseph and Choudhury, Romit Roy. “Hiding stars with fireworks:

Location privacy through camouflage." Proceedings of the 15th annual international conference on Mobile computing and networking, New York, NY: ACM, 2009. Print.

Munster, Anna Marie. "Data undermining: the work of networked art in an age of imperceptibility" Networked: A networked book about networked art. Eds. Green JA; Hankwitz M; Mancuso M; Navas E; Thorington H. Turbulence.org. Jan. 2009. Web <http://munster.networkedbook.org/data-undermining-the-work-of-networked-art-in-an-age-of-imperceptibility/>

Navas, Eduardo. "Traceblog," in Net works: Case studies in Web art and design. Ed. Burrough, Xtine. New York: Routledge, 2012. 127-42. Print.

Schulze, H. and Mochalski, K. Internet Study2008/2009, IPOQUE Report. <http://www.ipoque.com/resources/internet-studies/internet-study-2008_2009>.

Steinberg, Dan. "How Much Time Needs to be Spent Preparing Data for Analysis?" Sailford Systems. n.p. 19 Jun 2013. Web <http://web.archive.org/web/20130714182249/><http://1.salford-systems.com/blog/bid/299181/How-Much-Time-Needs-to-be-Spent-Preparing-Data-for-Analysis>

Zer-Aviv, Mushon. "Conflict of Interface". The Politics of Interface and Obfuscation. Eyebeam NYC, 34 35th St., Unit 26, Brooklyn, NY, 11232. Mar 11, 2014. Public presentation.

This publication has been supported in part by a grant from the Research Grants Council of the Hong Kong Special Administrative Region, China (Project No. CityU 21401114)