The Fibreculture Journal
DIGITAL MEDIA + NETWORKS + TRANSDISCIPLINARY CRITIQUE

issn: 1449-1443

FCJMESH-006
From Information Activism to the Politics of Data.

Maya Indira Ganesh and Stephanie Hankey
Tactical Technology Collective

Tactical Tech has a decade of experience supporting the use of information and digital technologies to support rights activism. They say that in this time they have witnessed a radically altered information eco-system thanks to an explosion of new technologies, a dramatic rise in technology uptake and a burgeoning government and corporate surveillance system. Here Maya Ganesh and Stephanie Hankey, from Tactical Tech, discuss their analysis of the challenges this new information ecosystem poses for rights activism and they describe the ways in which Tactical Tech are choosing to address these challenges.

doi: 10.15307/fcj.mesh.006.2015

As an organisation that supports activists and journalists to secure their communications to be more effective and more secure, we believe we have some parallels with groups working on a rather different issue: climate change. Environmentally friendly and sustainable lifestyle behaviours often start with having to recognise the easy short cuts and deeply ingrained habits we've gotten used to. Avoiding these short cuts and habits is something that many people invest a great deal of time and effort in when they do things like recycling, eat local produce or use a mobile app that tells them how to be a more ethical consumer. Climate change activists have developed a raft of inventive techniques to convey the message that

many aspects of how we live are damaging the environment and that we should change these practices. At the same time, many people find this message challenging because they believe it seems too difficult to shift entrenched practices.

In our work at Tactical Tech we're trying to do something similar. We're raising awareness around day-to-day behaviours—specifically digital practices and technology choices. However, we're trying to do this at a time when digital networks and interfaces have never been more seductive: smoother, faster and far-reaching. With minimal effort we can share a video, voice our opinions, have flowers delivered half-way across the world, or access government data. The digital is as opaque as a magic trick; and the magic is in how the messiness of cables, trade, policies, digital workers, and politics are seemingly made to disappear behind a facade of frictionless sharing.

By asking what the flip side of frictionlessness sharing is, we are advocating for the opposite. We're trying to convey to activists that the excitement and ease of communication, self-expression and sharing enabled by the digital, often erodes freedom of expression, human rights, personal liberties and people's right to privacy. We ask the people we work with to rethink their digital habits and to consider more difficult choices. The thing is, very few people really want to do that.

Then and Now

Tactical Technology Collective started its work in 2003 to promote and build the capacity of NGOs, journalists, bloggers and activists to use free, libre, and open source software (FLOSS) and technologies in their activism and advocacy campaigns. At this time, the "Microsoft model" of computing was popular: the computer was a fixed device connected to the Internet with cables, where users paid companies such as Microsoft to run proprietary software. We also advocated for the use of digital tools in information activism: collecting and curating information to monitor corporations, powerful social institutions and state actors, holding them accountable while promoting local and global activism. Tactical Tech has also worked with activist communities in different countries to use digital tools to identify and evade targeted surveillance by governments threatened by freedom of speech.

In the ten years since Tactical Tech began operating, Apple's market value has come to surpass Exxon Mobil's and the Internet is now heavily influenced by what we would term the "Google model": where every digital device and user has its facsimile in distributed data storage facilities (commonly referred to as "the cloud") [1]. Additionally, the Snowden leaks in 2013 revealed deep and pervasive collusion between corporations and governments to enable the surveillance of Internet users; we learnt that technology companies and the governments that regulate them, have developed an obsessive compulsion to collect and store data that most Internet users would deem personal or private. These conditions make the practice of and education about digital security, challenging. In an environment of mass surveillance, how is it possible to enable security and privacy measures if every digital act can be traced back to you, and with ever increasing levels of detail?

As a result of this environment, our work now encompasses the politics of data. Much like our early 'FLOSS-ophies' based on the merits of free, libre, and open source, the politics of data encompasses the technical, political and economic implications of the use of digital technologies. Our work in the area of supporting digital privacy rights is about encouraging awareness about risks and supporting activists to make different digital choices that resist, challenge or subvert the status quo; however, we're trying to do this at a time when the digital environment provides a host of ever-new and inspiring opportunities for activism.

Data everywhere

New media technologies are creating and collecting data about everything we say and do, which forces us to rethink how we present ourselves. There is information we know we're sharing about ourselves; there is information being generated about us that we do not create; and information about us is generated—unbeknown to us—simply because of our connections to other people online. These three kinds of information are being generated through digital activities and have been shown to compromise the security and privacy of activists, who have to rapidly develop new tactics of technology use in order to control their information flows.

In order to use the Internet now, different kinds of data are necessary to provide the services we've taken for granted: an identity, a location and a channel of communication. Whether using a real name or pseudonym, an email account will still be the key to a number of online services you may register for and therefore will provide a connection to your actions; this kind of chain of association means that eventually, you are always

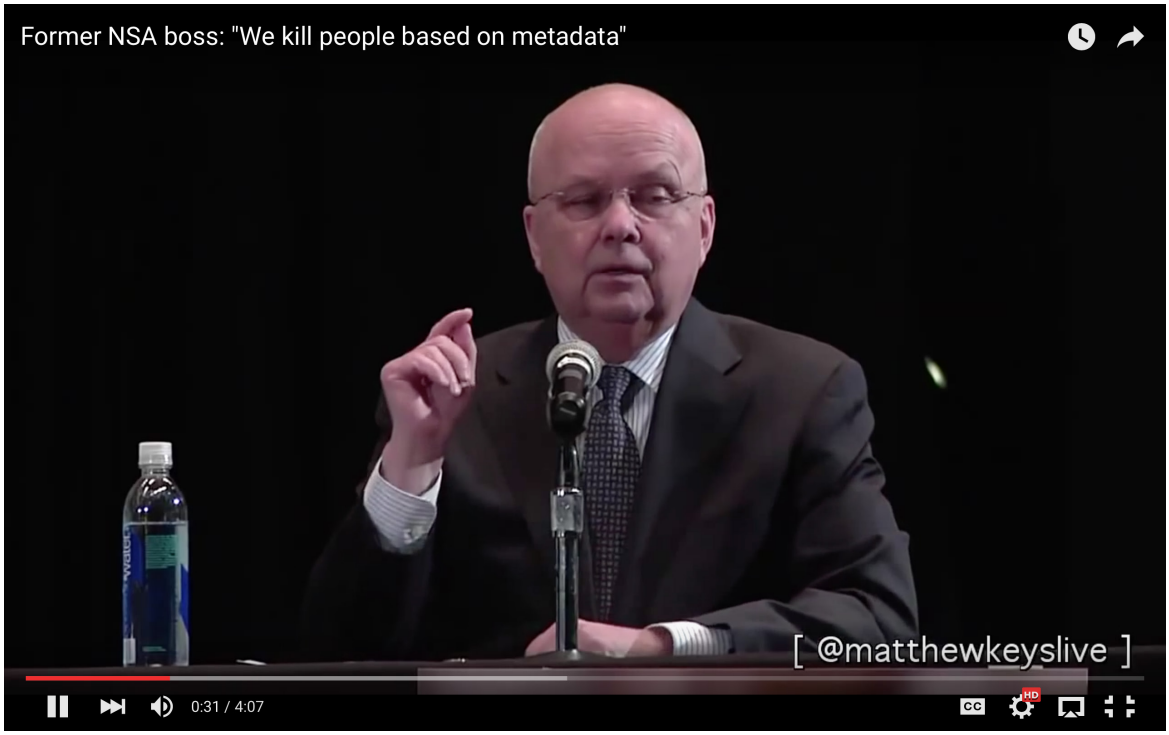
identifiable. Your location will also give you away: even if you never enable GPS on your digital device, using a service like Gmail or Facebook will give you a location that may not be physical—it may be in a network of people or based on where you travel online through linked services or even just your IP address that all these services log. Similarly, the channels we use to connect to the Internet, like ISPs, access points and service points, collect, store and relay information about users. This means that to completely avoid leaving behind data traces that can reveal our whereabouts, behaviours, and opinions, we need to consider, change or at least re-assess every single digital choice we make.

The kinds of personal behaviour changes we believe are required to minimise digital traces at Tactical Tech include choosing non-commercial or open source alternatives for everything from email to social networking, employing circumvention technologies and opting out of participatory practices associated with the 'sharing economy' [2]. However, we know that there are NSA and GCHQ programs designed to find and store information on users of the circumvention tool TOR and other privacy enhancing technologies. Even if we use tools designed to allow us to access or exchange information privately, we are rendered visible because of how out-of-the-ordinary our digital actions are. Also, many of these tools are difficult to use and install for those who don't have technical support.

The traces we leave and the way these can be used are extremely complex, particularly for activists. For example, during 'Operation Pillar of Defense'—the 2012 Israeli attack on Gaza—the well-known Egyptian activist Alaa Abd El Fattah tweeted certain views regarding Zionism. These tweets were later taken out of context and interpreted as 'calling for the murder of a critical number of Israelis.' This led to Abd El Fattah being stripped of the Sakharov prize in 2014, an award that acknowledges those who have defended human rights and freedom of thought. In a detailed response clarifying the context of the Twitter conversation, Abd El Fattah remarked, 'to pretend that you can interpret this tweet two years later without consulting the people involved in the conversation and to claim that it constitutes a call to action, is simply ridiculous.' Even as social media give us unprecedented reach and voice, what we do online can be accessed and used in ways beyond our control.

The struggle to control digital traces was also an issue for activists in the Hong Kong protests of late 2014. In this case the challenge was managing and making the right decisions about dual needs for anonymity and visibility. For those protestors who had been underground for many years prior to the street protests, it was important to remain undetected; however, the protests also provided an opportunity for these movements to become more active and potentially more effective. The choice to become actively

involved risked complete exposure, partly due to how our digital traces never really disappear. Activists in Hong Kong were also targeted with spyware and had their websites attacked.



(A youtube video is embedded in the online version of this paper - you can find that video at https://www.youtube.com/watch?v=UdQiz0Vavmc) Figure 1. Haydn, Matthew. 'Former NSA boss: "We kill people based on metadata"', Youtube, published 11 May, 2014.

These examples help convey the complex information ecosystem activists now inhabit. In using online services and platforms in our work and everyday lives—whether we think about it or not—we are knowingly giving away data about our actions in exchange for free services and this has consequences and repercussions that may take years to unfold.

In many cases the data that leaves the messiest and least visible traces is metadata: information about all the information we create and consume. Metadata is an invisible layer of information on digital photos, in the logs of wifi access points—which also record all the other wifi points users have connected to over the previous 30 days— including call durations and times of phone calls. The power of metadata, often considered mundane and ubiquitous, became apparent when the former director of the NSA and CIA, Matthew

Haydn (2014) remarked, 'we kill people based on metadata' during a dialogue about the practice of mass collection of communications information (see Figure 1).

Current debates about metadata often neglect to mention that it does not need to exist: that it is built into systems and products. News of end-to-end encryption of Whatsapp, the Facebook-owned instant messaging service, was received with enthusiasm for privacy adoption by commercial services; however, whilst the content remains obscure, the metadata associated with instant messaging—who messaged who, when, and how often—is still seen by Whatsapp, and therefore by Facebook, and could still be accessible to government agencies with the capacity to read and analyse it.

Moxie Marlinspike, the founder of Open Whisper Systems that partnered with Facebook to encrypt Whatsapp says that the change is 'nearly invisible,' that '[o]rdinary users won't know the difference,' and that '[i]t's totally frictionless' (cited in Greenberg 2014). Marlinspike's evocation of frictionlessness emphasises the problematic idea that what is sold as efficiency and smoothness, ends up concealing how things really work. Integrating encryption into commercial software can be seen as a positive step, as it will help normalise the practice; however, a frictionless approach moves to obscure the complexities of privacy issues. Users may become complacent about the metadata attached to their encrypted messages and the companies who aggregate and analyse this information.

Enabling awareness, alternatives, and action

According to the security expert Bruce Schneier (2014), since Edward Snowden leaked information about the NSA's and GCHQ's mass surveillance programs, 700 million people worldwide have taken steps to be more private in their communications. Through our work at Tactical Tech we see a small slice of what this means for activists; an increasing demand for training, support and an increase in the number of people accessing our online digital security toolkit from 417,000 users in 2012 to 2.5 million by the end of 2014.

One of the challenges in raising awareness about the new Internet we inhabit is that most users don't have the right metaphors or mental models to even comprehend its scale and velocity. Mental models affect how people choose to accept or reject information about the environment around them and their own role in influencing events. Design researcher, John Fass, is working on mental models of computing and draws on work by Evgeny

Morozov who shows how hazy and misleading metaphors of how the Internet works are: the cloud, the Chinese 'fire-wall' and the cold war are thin metaphors that give misleading information about the material, political, and social realities of computing and Internet governance.

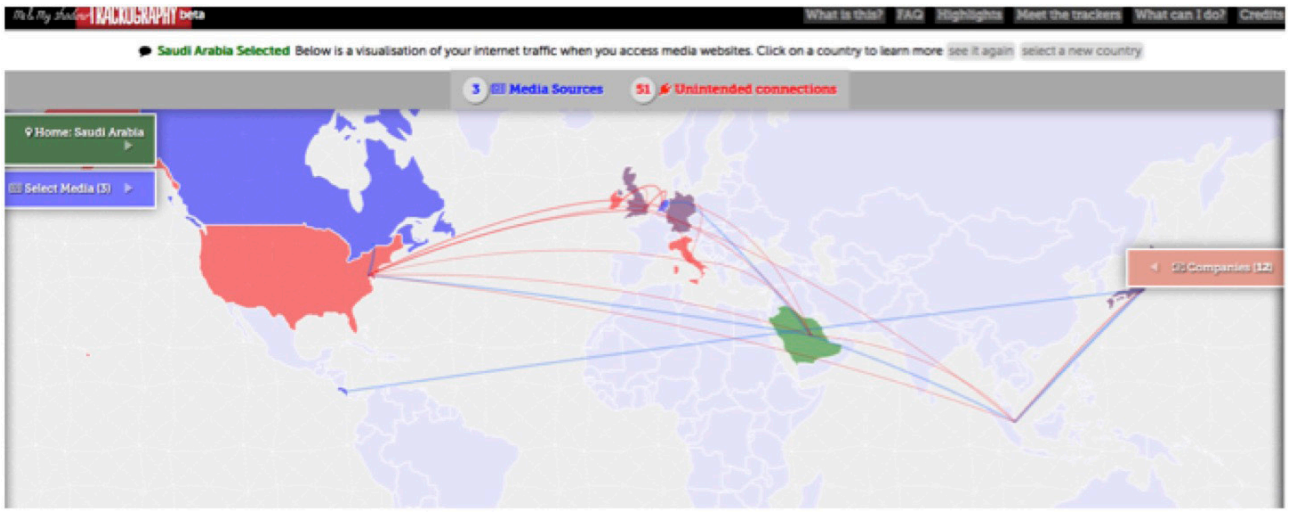


Figure 2: Screen grab of Tactical Tech's new project Trackography that reveals the third parties that have access to information about the news sites you visit online. Launched in December 2014, Trackography visualises data from news media websites and blogs in over 30 countries.

These metaphors are confusing and affect activists' ability to discard old behaviours and take on new digital practices. At Tactical Tech we have witnessed this in training workshops, from having to break the news that there really is no cloud in the sky that makes the Internet work, to making visible—in the form of dynamic visualisations—the data we give out from our devices as we move around a building, a city or a country. These mental models also compete with the slick narratives and metaphors about technology promoted by advertising and marketing of technology devices. Awareness raising and education also come up against some known arguments, like 'I have nothing to hide' or, 'I don't like it, but surveillance is required for national security.'

We try to take on these challenging, difficult arguments with strong evidence and convincing counter-arguments, or at least find the "sweet spots" that may serve to shift peoples' understanding of the problem. What is difficult about this is that we are saying to activists, in effect, that they have to limit, stop, or re-evaluate their own desires and practices online: that the biggest challenge is shifting their own behaviours. All we

can really control are our own practices, and this is challenging as digital and mobile technologies have revolutionised how activists can use information in campaigning and in their personal lives.

Learning from the Climate Change movement

Advocating for and raising awareness about privacy and digital security for activists, is starting to mirror the climate change movement in certain ways. This involves developing scenarios about unseen, unknowable problems that deplete existing resources and erode peoples' power—in this case freedom of expression and democratic practices. We cannot conclusively prove these* *future scenarios, but the abundance of evidence outlining current problems can be used to develop new methods to communicate to a broader audience.

The climate change movement has successfully encouraged individuals to take small steps to change their practices in favour of more sustainable ones. This has included actions like recycling and switching off the lights; in our scenario, we seem to be left with the individual acts of changing our privacy settings or not tagging friends in Facebook photos. However, it is clear in both the climate change and Internet freedom movements that these small steps, even in aggregate, are not going to make a dent in the system. Eventually, it is up to corporations and governments to make important new policy decisions and commitments. This is not likely to happen in any near future, however, as with climate change action, it takes people opting out, voting with their feet and choosing companies with better track records in order for viable alternatives and new markets to emerge; as with climate action, this can result in companies and governments feeling pressured to enact regulations, as opposed to talking about self regulation. For this reason, some of our new advocacy work is about using information technologies for transparency to reveal the workings of the data industries. Challenging the opacity of narratives, metaphors, and the workings of the data industries is one way to advocate for a change in digital habits and practices.

Still we are left asking: is it possible to inspire individuals to change their digital practices? We remain hopeful and concur with this statement made by investigative reporter Julia Angwin, author of the 2014 book Dragnet nation: a quest for privacy, security and freedom in a world of relentless surveillance [15]:

We lived in a world where we were perfectly willing to tolerate our rivers catching fire and the air being filled with soot and people dying of black lung disease and then all of a sudden, after 50 years of that, we decided maybe we don't want that kind of world. And we've been very successful at cleaning up our environment. We did it partly through laws, but we also did it by changing our social norms. I think privacy is a similar social problem. It's something that we will change both through laws and also through being smart about what choices we make about what technology we use. (Julia Angwin 2014).

Author Biographies

Maya Indira Ganesh is Director of Applied Research at Tactical Technology Collective. She led the 'Evidence & Action' Program 2011–2014 where she worked on writing the Visualising Information for Advocacy book and helped develop the Info-Activism Camp in 2013. Before joining Tactical Tech, Maya worked on one of the first studies of gender and online violence with APC's Women's Rights Program and on ICTs in development. Maya holds Masters degrees in Applied Psychology from Delhi University, India, and in Media and Cultural Studies from the University of Sussex, UK. She is persistent in her attempts to write consistently but is usually distracted by Twitter.

Stephanie Hankey previously worked with the Open Society Institute establishing their Technology Support for Civil Society Program, before co-founding Tactical Tech in 2003 and Tactical Studios in 2011. Stephanie has a background in information design, was editor-in-chief of Pulp magazine and worked as a creative director and producer for a number of London-based multimedia companies. She has a Masters in Information and Interaction Design from the Royal College of Art London and a certificate in Campaigning and Lobbying from NCVO. Stephanie is currently developing Tactical Tech's work on influence and visual persuasion and leading its new initiative on data shadows and political engagement.

Acknowledgement

We would like to thank Marek Tuszynski and Bobby Soriano for their inputs.

Notes

[1] This is a business model that has profited a number of different technology companies; Google is just the biggest and most prominent of these. More details about NSA and GCHQ surveillance programs enabled by mass data collection can be seen here: https://projects.propublica.org/nsa-grid/

[2] The sharing economy (sometimes also referred to as the peer-to-peer economy, mesh, collaborative economy, collaborative consumption) is a socio-economic system built around the sharing of human and physical resources. It includes the shared creation, production, distribution, trade and consumption of goods and services by different people and organisations. This definition is drawn from http://en.wikipedia.org/wiki/Sharing_economy.

References

Angwin, Julia. Dragnet nation: a quest for privacy, security and freedom in a world of relentless surveillance (New York: Times Books, 2014).

Greenberg, Andy. 'Whatsapp Just Switched on End-to-End Encryption for Hundreds of Millions of Users', Wired Magazine online edition, published 18 November 2014, http://www.wired.com/2014/11/whatsapp-encrypted-messaging/

Haydn, Matthew. 'Former NSA boss: "We kill people based on metadata"', Youtube, published 11 May, 2014, https://www.youtube.com/watch?v=UdQiz0Vavmc

Schneier, Bruce. 'Over 700 Million People Taking Steps to Avoid NSA Surveillance', published 15 December 2014, https://www.schneier.com/blog/archives/2014/12/over_700_millio.html