The Fibreculture Journal
DIGITAL MEDIA + NETWORKS + TRANSDISCIPLINARY CRITIQUE

issn: 1449-1443

FCJ-195 Privacy, Responsibility, and Human Rights Activism

Becky Kazansky
Tactical Technology Collective

Abstract:

In this article, we argue that many difficulties associated with the protection of digital privacy are rooted in the framing of privacy as a predominantly individual responsibility. We examine how models of privacy protection, such as Notice and Choice, contribute to the 'responsibilisation' of human rights activists who rely on the use of technologies for their work. We also consider how a group of human rights activists countered technology-mediated threats that this 'responsibilisation' causes by developing a collective approach to address their digital privacy and security needs. We conclude this article by discussing how technological tools used to maintain or counter the loss of privacy can be improved in order to support the privacy and digital security of human rights activists.

doi: 10.15307/fcj.26.195.2015

Introduction

Tactical Technology Collective (Tactical Tech) is an international Non-Governmental Organisation focused on supporting the effective use of information in advocacy. Tactical Tech has spent a decade listening to, documenting, and responding to activists' privacy and digital security needs and challenges across the world, often in contexts where the free flow of information is constrained. This vantage point has allowed Tactical Tech to observe the transnational spread of digital surveillance technologies, and their use against human rights activists (Hankey and O'Clunaigh, 2013; Notley and Hankey, 2013). Stories of monitoring and intrusion facilitated through digital surveillance technologies have been relayed to Tactical Tech in training events, through research and documentation field trips, at conferences and workshops, and via networks and activist media. These stories confirm the kinds of harms described and theorised in surveillance studies literature and in reports by civil society organisations documenting the psychological effects of mass surveillance, such as anxiety (Bigo, 2006), 'anticipatory conformity' (Braman 2006, 130), and 'self censorship' (Human Rights Watch, 2014; Pen America, 2013). These stories also confirm that human rights activists are often made key targets for surveillance because they challenge powerful interests, expose injustices and make rights claims in repressive environments, while they also provide evidence that surveillance can end in physical harm or arbitrary and unjust imprisonment (Citizen Lab, 2014).

Despite the substantial risks they face, human rights activists, like all 'users' of networked technologies, are tasked with the responsibility of managing their personal information in a way that supports privacy and security. We use the terms 'privacy' and 'security' throughout this paper in a complementary fashion. Privacy refers to the anonymity and confidentiality of information shared and stored through devices such as phones and laptops, and through digital platforms such as Facebook or Google. 'Digital security' refers to the concrete strategies or actions that respond to or resist a lack or loss of privacy; this involves the development and/or implementation of practices that can enhance anonymity or ensure confidentiality while also mitigating the consequences of data loss and intrusion. Overall, or 'holistic security'(Tactical Technology Collective, 2014) in human rights work is contingent upon the use of strategies for managing information which tie privacy to the physical protection and wellbeing of human rights activists.

One challenge human rights activists face in designing and implementing digital security strategies is that simply starting this process requires substantial technological knowledge. Like all users, protecting their privacy requires that they understand the properties and extent of 'data traces' left behind when using online consumer services and software; that they know the complex legal rights they have through commercial platforms' Terms of

Service (TOS); that they be able to manage the technological options available to change default user settings; and that they are able to apply additional technological remedies to compensate for the lack of protection or control such platforms provide. The additional high level risks and threats posed by contemporary digital surveillance and intrusion in the context of human rights work also demands that concerned activists learn how to investigate potential data leaks from their devices and those of their colleagues, friends or personal networks. Yet this is a complicated endeavour: activists and human rights organisations often have limited technological support, while sophisticated surveillance attacks are so complex that only a tiny cadre of digital forensic experts are able to investigate with certainty whether a device has been technically compromised or not.

As part of our work supporting the digital privacy and security of human rights activists, we undertook field research during the period October 2013 to November 2014 to better understand how capacity building interventions such as digital security trainings figure into constructive responses to surveillance, privacy breaches, and overall security concerns in human rights activism. This research, part of our 'Security in Context' research project looked specifically at what factors cause concern over privacy and security to first arise, how digital security practices spread between individuals, groups, and networks, and how trainings aid these trajectories of awareness and learning. This work was founded on Tactical Tech's belief that issues around privacy and security must be engaged within a contextually appropriate way (Tactical Technology Collective and Front Line Defenders, 2015). To meet this aim, our capacity building efforts, such as the trainings that we conduct, start with a 'context analysis' of social, political and technical factors affecting human rights work at a particular place and time. This process serves to bridge knowledge of relevant threats between training facilitators and participants. Following this form of assessment, strategies are created and tools are chosen based on an emergent mutual understanding of the most salient concerns. This training approach directly informed the mixed method approach of our research, which utilised surveys, semi-structured interviews, workshop-based discussion and participatory activities with a total of 40 participants based in four different countries.

Reporting on some of the findings from this study, this article highlights the experiences of a network of women's and LGBTQI rights activists who set out to address their privacy and security concerns collectively in order to counteract digital surveillance, online harassment, threats of physical violence, and in some cases, physical violence. Because the use of Facebook has figured so prominently in their work, we focus on Facebook in this article as a platform for organising, as a technological interface with a certain set of properties or affordances which affect the kinds of control available to a user concerned with privacy, and as a company with policies that reflect a particular culture and business model. Our research finds that while Facebook was invaluable to the activists for organising protests

and actions and later in creating strategies of self-defence, this platform also proved to be one of their greatest points of vulnerability. Already challenged by a large resource differential between themselves and their opponents, this imbalance of power was compounded by activist's forced reliance on an opaque, commercial platform offering little protection or control to its users. We call this a forced reliance because Facebook, as a networking platform, facilitates the maintenance of existing social ties and serves as a popular and dominant channel through which new relationships are created and sustained, and because there is no comparable replacement available. Baumer et al (2013) describe this forced reliance as a form of 'lagging resistance' wherein users express high levels of dissatisfaction with a tool but ultimately continue to use it for lack of viable alternatives. The phenomenon of lagging resistance demonstrates a systematic failure to provide users with adequate choices, protections, or controls over their privacy.

Digital Privacy and Responsibility

Conflicting views among software developers, activists, and policy makers reflect ambivalence over where primary responsibility for the protection of privacy should lie. Free Software luminary Richard Stallman starts his article titled 'How Much Surveillance Can Democracy Withstand?' (2014), by admonishing: 'First, don't be foolish. To have privacy, you must not throw it away.' Stallman's view reflects an expectation that users assume control and exhibit common sense in their actions using online tools. Stallman then outlines steps for users to take back control of their data, but goes on to admit that 'self-protection is essential, but even the most rigorous self-protection is insufficient to protect your privacy on or from systems that don't belong to you.' What kind of control users can realistically take in light of the complexity of risks, lack of meaningful alternative choices, and lack of accountability by companies, becomes the ongoing question for those creating privacy enhancing technologies or advocating strategies for greater privacy and security.

For activists working to defend human rights, it can be difficult to reconcile the need for and demands of self-protection with the feeling that the nature of their work should not require having to adopt a vigilant, self-defensive posture. One women's rights activist we interviewed, who, in her use of Facebook faces regular harassment and hacking attempts by a concerted collusion between state and state-affiliated actors, explained: 'I want people who are doing things that are making me digitally insecure to not do those things. I feel a tension in having to assume that responsibility.' [1]

The process through which technology users are granted primary stewardship over

their digital privacy has been characterised by scholars working on privacy enhancing technologies as a form of 'responsibilisation' (Gürses, 2014; De Wolf, Heyman and Pierson, 2014). They enter into a dependent relationship with opaque technologies, and are effectively left no choice but to deal with ensuing threats individually. The term responsibilisation originates from an interrogation of the privatisation under way in the 1980s in the United Kingdom and the United States, and the neoliberal discourse which validated and rationalised it (Shamir, 2008; O'Malley, 2009). Iyengar (1989) studied the societal effects of arguments for the disbandment of social services, finding that a prevalence of discourse punishing dependency on social services had profound effects on individual attitudes towards societal problems. Encouraging an emphasis on the individual as the primary locus of responsibility for protection from harm had the convenient effect of deflecting attention from its causes. Garland (1996) characterises the increased displacement of responsibilities onto individual citizens as 'a new form of governance-at-a-distance.' Similarly, D. Barnard-Willis and D. Ashenden (2010), who looked at the United Kingdom's recent efforts to frame online identity management as an individual responsibility, characterise responsibilisation as a mode of 'directing of conduct'. Surveillance studies scholar Mark Andrejevic (2005) describes responsibilisation as an evolving strategy of governance that encourages self-management and self-policing through technologically enhanced 'peer-to-peer' monitoring tactics and tools such as online social networking platforms.

Discourses and processes of responsibilisation figure prominently in current frameworks for privacy regulation. The Notice and Choice paradigm is a prime example. Solove (2012) characterises the Notice and Choice paradigm as a form of 'privacy self-management,' whereby users are, in effect, tasked with both the job of understanding the consequences of choosing platforms such as Facebook, and with protecting themselves from subsequent harms of their data collection practices on their own. Upon the first use of a commercial service, a user is presented with 'notice' in the form of a Terms of Service agreement (TOS) enumerating the privacy policies, rights, and responsibilities governing the platform, with 'choice' provisioned through a small checkbox at the bottom for a user to signify consent to or denial of the terms. However, the 'notice' provided by TOS agreements cannot guarantee meaningful transparency to an individual user. For example, an individual user will rarely learn that governments requested access to their data, as the disclosure of this information is supervised in secret court rulings (Facebook, 2015a). Nor do TOS guarantee that as a company's business model finds new uses for its users' data, what was previously protected won't now be exploited (FTC, 2011). The most consistent element of Facebook's privacy policies is just how often they change to take advantage of new business 'use cases' for data (Hill, 2014). Thus the notice to users provided is vague or limited, while at the same time setting forth the expectation that the user has been educated enough to now make decisions in their best interest.

As for 'choice', though the Notice and Choice paradigm of consent appears to offer users a form of empowerment through the provision of choice, a user's denial to the stated terms precludes further use of the platform. This is a false choice in an environment where no alternative exists aside from 'opting out' (Barocas and Nissenbaum, 2009), especially since opting out may not be seen as a choice by human rights activists, for whom popular platforms such as Facebook are critical to reaching broad and target audiences in their work. Further, the act of providing consent in one isolated instance grants easy access to personal data to 'third parties' 'downstream' (Solove, 2006), much of it covert and unknown to the user, such as in the sweeping up of user data by local law enforcement, by globally-operating intelligence agencies (Meyer, 2014), or in its sale to 'data brokers' (Ohm, 2010). Consent given through Notice and Choice thus becomes an 'artificial procedural justification' offering a 'wild' card to companies as to what can be done with the data now and in the future (Ausloos, 2012). That Notice and Choice in actuality provides very little 'notice' or 'choice' means this paradigm of privacy protection merely provisions a pretence of control. Having provided content to a platform to use data in both known and unknown ways, users who want 'instrumental privacy'—which we define as an assurance of confidentiality of personal information on platforms such as Facebook—are left to take practical steps that may result in varying efficacy. Capacity building efforts such as digital security trainings, which aim to increase the efficacy of privacy practices, must also respond by compensating for the false promises and opaque statements that are embedded into different platforms models of privacy protection.

Because the Notice and Choice model is used so widely in commercial platforms, it follows that its use has an effect on the privacy of many different kinds of users, including those engaged in human rights activism. The roots of this model may help to explain its failings while also raising flags in regards to how it may shape norms outside its initial sphere of influence. Notice and Choice can be understood as the product of the United States' particular conception of consumer privacy, heavily influenced by commercial interests and built on a case-by case basis in courts, with limited regulation by bodies such as the Federal Trade Commission. The loosely governed approach in the United States is often contrasted with the European Union's more systemic framework, which employs the concept of 'data protection,' as laid out in the European Data Protection Directive (Directive 95/46/EC) in 1995. Despite the EU's protectionist framework, with its granular data collection and processing guidelines and restrictions, both conceptions have roots in the Fair Information Practice Principles of the 1970s (Solove, 2009), and the EU framework continues to rely on the Notice and Choice paradigm. This is significant, considering that the EU Data Protection Directive is increasingly looked to as a standard for countries outside the EU to emulate (European Commission, 2014).

Applied within Facebook, Notice and Choice serves to reinforce the culture and practices of the company. Facebook's origin is in an experimental website called Facemash, created by Mark Zuckerberg in 2003 to rank the looks of students with ID photos stolen from a university database. It was soon shut down due to outrage over Zuckerberg's exploitation of this data and his disregard for consent (Harvard Crimson, 2003). In his next experiment, Zuckerberg developed the first prototype of the Facebook platform as users know it today. Facebook's TOS and interface have since undergone countless permutations, but Zuckerberg's ideas of privacy and online identity have continued to loom large. In 2010, Zuckerberg now famously told the author of the Facebook Effect (Kirpatrick, 2010) that 'you have one identity,' and 'the days of you having a different image for your work friends or co-workers and for the other people you know are probably coming to an end pretty quickly.' Five years since he made this statement, Facebook's 'real name' policy remains intact, though harms to vulnerable users like human rights activists have been well documented. Today, Facebook's user base has expanded far beyond the platform's original intended audience of college students with the majority of its one billion plus users today residing outside the United States. Some of these users are involved in social movements and human rights activism and these uses are also far outside the experiences of Facebook's creators. As one women's rights activist we interviewed put it: 'It's really not a tool built for activism and yet we use it, because we were on Facebook first and then people decided they wanted a revolution, so they organised through there.' [2]

Facebook's application in ways not anticipated by its creators produces the sort of 'frictions' discussed by Anna Tsing (2005) in *Friction: an Ethnography of Global Connection*. For Tsing, the global movement of ideas, people, and goods produces global paradigms that transcend local discussions while obscuring their origins. Though Facebook and the Notice and Choice model have a 'global' reach and impact on privacy norms—in that their uses circulate through transnational market flows, federated communications protocols, and fibre optic cables connecting the world—this does not tell us what effects they have on the privacy of people in any particular context (Nissenbaum, 2009). It follows that we can learn about the impacts of technologies and legal frameworks by documenting the frictions that result as these frameworks and technologies are applied in unanticipated ways in specific contexts. In the following section, we examine how the Notice and Choice paradigm and its use by Facebook shape the experiences of a particular group of human rights activists. This case highlights some of the most widely observed challenges in developing strategies for privacy and security in human rights activism which resonated across the 40 interviews we conducted, while also illuminating new directions for strategies and remedies. In light of privacy and security concerns and in agreement with the activists we interviewed, we have determined that the only way to share their stories is by removing names, geographical details, and other unique identifiers.

Threats, in Context

As part of our Security in Context research project, we interviewed and facilitated a workshop on privacy and digital security with 16 women's and Lesbian, Gay, Bisexual, Transgender, Queer, Questioning and Intersex (LGBTQI) rights activists. These activists, representing several different organisations who work together through an informal network, described how, over the course of nearly a decade, their work has become increasingly dangerous, to the extent that they now face significant personal, organisational, and network-wide risks in continuing to pursue it. About a year before our interviews, one of the organisations received an anonymous threat in a message sent on Facebook, to cease work on women's rights and LGBTQI issues or face having their office bombed. Soon after, members of a nationalistic group assaulted several of the women's and LGBTQI rights activists physically at a protest. Additionally, around the same time, anonymous harassers began using one of the organisation's media materials and personal Facebook photographs to create videos claiming the activists were responsible for destroying traditional family structures through their focus on women's rights. The misinformation campaigns often included messages culturally equivocating the words 'gender' and 'LGBTQI' with 'paedophilia'. For the activists, there was no clear way to respond:

> *They used my photos, they exposed my personal contacts, and we couldn't reach the creator of the video because it was done in an anonymous way. We asked ourselves, what are the next steps we need to do? [3]*

These campaigns and threats of violence appeared to emerge from an organised collusion between nationalist groups and governmental actors, part of a larger effort to marginalise women's and LGBTQI rights said to be motivated by the brokering of an important economic union with a much more economically and culturally powerful neighbouring country. The network of women's and LGBTQI rights activists heard from several sources that this neighbouring country had sent officials to train local media in how to wage these campaigns, as part of a broader effort to exert their cultural influence. The network felt these campaigns were successful in changing public perceptions in a way that has impacted their ability to safely continue to push for women's rights.

Amidst these developments, the network gained information that the neighbouring country was also tapping into phone lines and Internet Service Providers and tracking social interconnections visible through online social networking platforms. Concern and anxiety over surveillance and intrusion were inflamed by stories of hacked websites and email

accounts, strange sounds heard when using Skype, and the presence of clicking noises when using the landline telephone. Though nearly impossible to know whether such phenomena are clear indicators of active surveillance, it was at least reasonably plausible given the consistency of more overt surveillance incidents such as regular visits and phone calls from local security agencies inquiring into the whereabouts of specific members. While this surveillance was a burden in its own right, there was also no proof that it was directly connected to the described attacks and misinformation campaigns; thus it was very difficult for the network to really define the source or sources of these threats and behaviours.

Before the violence and threats of violence began, the network felt a strong public presence, and thus a visible online presence, was vital to the success of their activism. The activists used their 'real', legal names in Facebook profiles, not just because Facebook's TOS states that users must do so, but because their profiles served as a public point of contact for those interested in joining their advocacy work. However, since the women's and LGTBQI rights network could now anticipate that a public presence and publicly organised actions might lead to more violence and harassment, they felt a need to use pseudonyms, and to generally be able to shape their identities as they saw fit. Facebook's rigid 'real name' policy became a clear point of vulnerability. They were thus forced to violate the policy in order to protect themselves.

Facebook's changing photo privacy settings also exposed the activist network to harm. Despite vigilance over privacy settings, personal photographs would find their way into new misinformation campaign videos. Upon having time to sit down and pinpoint the source of the leak, the activists found that the settings controlling the visibility of photographs had again been changed by Facebook. The harassers exploited this change to obtain new materials for their campaigns. After this incident, many activists simply deleted sensitive photos rather than risking further exposure. The activists learned to review their Facebook privacy and account settings on a regular basis due to this incident, but were still shocked to discover over the course of a workshop provided by Tactical Tech that once again, photographs previously visible only to friends had unexpectedly become 'public' without any actions taken on their part. Instead, this change could be attributed to Facebook itself.

Responding to Threats

Despite the unexpectedness of the threats and attacks—and their heavy toll—shared experiences of harassment and attacks brought the activists closer. Several individuals and organisations came together to form a more cohesive network, out of a shared need to be more strategic in countering threats: 'Much of our understanding of safety is about reaching out to other people instead of relying on our selves. We need to be able to rely on community'. [4]

The network agreed to make public appearances together from this point forward, and they implemented a new office-wide physical security policy. They also set up a secret Facebook group (Facebook, 2015b) in order to document security incidents such as online harassment and attacks at protests. For the activists who administered it, the main draw of the secret group function was that such groups are only visible to explicitly invited Facebook users (Facebook, 2015c). This form of documentation allowed the network to quietly but collaboratively track patterns in their harassers' behaviours. It became apparent that the 'online' and 'offline' harassment they experienced shared a similar tone and language, which allowed them to establish links between these behaviours. One activist who spearheaded this effort described first hearing the idea of documenting security incidents during security training, about a year before the attacks. At the time, he couldn't find the immediate relevance of this advice, but the attacks changed his understanding of protection:

> *Before the attacks I felt it was more important for people not to worry than to know about threats [made] on Facebook. I was keeping secret from everybody when I was receiving threats on Facebook. I used to delete them. I thought it was protection if they didn't know. [5]*

The use of Facebook secret groups, shows how the social network of activists facilitated joint ownership of security. Still, there was a clear friction here between Facebook's affordances and the activists' needs. Almost all those using the Facebook secret group function questioned the groups' true level of confidentiality. Though secret groups are invisible to uninvited Facebook users, the groups and the material they post is visible to Facebook and potentially to third parties who work with Facebook, as well as anyone else who gains access to the accounts of group members. A breach of any one account would expose the highly sensitive communication of the entire secret group. A fear persisted that even if information was not made public, opponents would find a way to get their hands on it: 'we are working in a secret group but how can we really know if it is closed or if some people can see our messages?'. [6]

As part of an evolving security strategy, the network began to use fake Facebook accounts to track the discussions and plans of their harassers, which took place in open and closed Facebook groups. This tracking enabled the network to prepare for possible harassment and violence at future protests, but the tactic did not remain effective for long. After using fake accounts to track the planning of a new attack, the network reported these planned actions to the local police. When word of this somehow got back to their harassers, the harassers closed these groups and moved on to create their own new fake accounts and secret groups, thus avoiding further tracking from the network. This tactical dynamic, which Gary Marx (2009) characterises as one of 'neutralisation' and 'counter-neutralisation,' demonstrates the constant evolution and interplay of 'online' and 'offline' monitoring, harassment, and violence, which resulted in the women's rights and LBGTQI network spending an increasing amount of time monitoring their harassers through social media, fixing privacy settings, and learning new security practices. Activists in the network said they reached out to Facebook in order to report the nationalist organisation they linked to online harassment, threats, and violence at protests. In response, Facebook sent them automated responses confirming the receipt of their report. Meanwhile, despite their efforts, the collective was not able to mobilise local law enforcement to interact directly with Facebook on their behalf.

It is clear from the limitations of both the network's individual and collective efforts that the load of responsibility the women's and LBGTQI rights network carried for their self-protection was too great to bear on their own. Though addressing privacy and security collectively proved enormously helpful in regaining strength and becoming more strategic in their activism, the network was continuously compromised by both Facebook's rigid identity management guidelines, frequently changing privacy policies, and general opacity. In their opinion, Facebook has not been accountable for the terms the company itself sets out in its Statement of Rights and Responsibilities. As a result of their experiences, the activist network has feedback they want to deliver to the company. They believe they deserve more of a response to threats and attacks than an automated reply, and that for the sake of their protection, they should be able to define and tweak their identities through the use of pseudonyms or other self-defined forms of identification. Though Facebook recently clarified that the 'real name' policy requires an 'authentic identity' rather than an actual legal name, the fuzzy, arbitrary distinctions between these signifiers only add to the opacity of the guidelines (Facebook, 2015c). Activists in the network also believe Facebook should make clearer the true extent of privacy and confidentiality offered by the secret groups, in which content is not kept secret from Facebook itself. Finally, members of the network point out that in the same way that they've now installed physical security cameras in their office to alert them to changes in their environment, Facebook should alert them more visibly to changes in privacy settings which affect the relative anonymity of their sensitive, personal information.

As for other structures that might be engaged for support, the network believes governmental actors should contribute to their protection. It remains unclear how direct a role their own national government played in their harassment and attacks, though evidence gathered by the network points to some sort of cooperation. One interviewee expressed scepticism in regards to the ability or intent of large supranational human rights structures to provide any concrete protection, due to a lack of economic incentives: 'the UN will not protect us. Human rights in this country are just about money'. [7] Meanwhile, the network felt that while local police were helpful as a form of protection at local protests, they showed no interest in investigating the links between 'online' and 'offline' attacks in a sustained manner. Finally, when we're told that there is a recently created cybercrime division in the national government to guard against new 'cyber attacks' and to push for more 'cyber security,' it is with an anxiety over what effects the accompanying new forms of surveillance or enhanced monitoring might have on their work: 'National security is one thing. Personal security is another'. [8] Clearly there is no single, cohesive governmental response that can address digital privacy and security on Facebook or across platforms. Rather, there are confusing, heterogenous structures for the activists to navigate, which in itself adds to the burden of their responsibilities.

Remedies

The experiences of the women's rights and LGBTQI network point to the need for a range of remedies. Those we discuss here relate directly to the perceived needs pinpointed by the activist network as they relate to the confidentiality of the messages they share with each other using Facebook. This discussion is informed by the high probability that many activists will continue to use Facebook, in spite of Facebook's shortcomings as a tool for human rights work. Of note, alternative online social networking platforms such as Diaspora and Crabgrass have existed for years, however, they were not used by the women's rights and LGBTQI network at the time of the attacks. Though Tactical Tech supports and promotes the use of alternative, open source tools and platforms, we also recognise the difficulty of 'migrating' to them from their commercial equivalents and thus we seek to mitigate the harms that can result from their use, while also demonstrating alternative options. The question, in light of a continued reliance on Facebook, is what ways exist to increase the amount of control available to users. This control becomes crucial for overall security, as the attacks on the women's rights and LGBTQI network showed that breaches in privacy can be linked with instances of physical violence.

In order to control access to all content in Facebook accounts, users may choose to add 'two-factor verification' through a Facebook feature called Login Approvals. This

feature provides an added layer of protection against weak or compromised passwords by requiring the use of a security code sent via sms to the user's cellphone in order to log in to the platform. Unfortunately this feature does not help with the confidentiality of communications once access to the account is gained or if messages are accessed through the account of one of the other correspondents engaged in conversation. To guarantee confidentiality of the messages themselves, users may turn to the use of Cryptography-Based Access Control Tools (Balsa, Brandimarte, Acquisti, Diaz and Gürses, 2014). The use of such tools can enable a user to take back some control over the level of confidentiality of their content, to the extent that a platform like Facebook, or potential opponent who gains access to a Facebook account, would no longer have the ability to read one user's messages to another.

Many of these tools, such as the 'chat clients' Jitisi and Adium, are free to use and readily available for download. Unfortunately, as Balsa, et al point out, they lack wide adoption. The experience of the women's rights and LGBTQI activist network is illustrative of some of the challenges of implementing such tools, helping to explain their low adoption rates. While the usability of tool interfaces has gained increasing attention in its importance as a barrier to tool adoption, we turn now to an interwoven but distinct issue that can override the usability considerations of the tool interface. Human rights activists are often motivated to master difficult tool interfaces. However, even when they do, through trainings or individually, they often have no one to use them with. To exchange encrypted messages, they must then take on the additional responsibility of spreading skills among colleagues or members of a wider network and in convincing them of the value of such digital security practices. Often this skill transfer doesn't take place because of constraints on time and resources, so that tool uptake remains limited to individuals with skills received via training or self-directed learning. This limitation points to a great need to more easily integrate digital security practices into the interactions of individuals and groups, both by optimising tools for use within groups and by facilitating more opportunities for learning within groups who are already engaged in communication with one another through online channels. As one interviewee told us, 'when it is about security of colleagues, the security becomes real'. [9]

Currently, the use of communications-based encryption is contingent on an exchange between two individuals, but for more than two people, this form of encryption can become exceedingly difficult to implement. In tools such as Jitsi and Adium, this is partially due to the specific cryptographic protocol implemented within them—called Off The Record Messaging (OTR)—though there is work being done to create a 'multi-party' version of OTR (Goldberg and Ustaoglu, 2009). In addition, Adium and Jitsi also cannot be used with Facebook's secret, closed, or public group utilities. Thus, these tools cannot mitigate the vulnerabilities created by the network's reliance on secret groups for group

communications. The betterment of these tools will depend on how tightly technical specifications and cryptographic implementations are bound to the consideration that security emerges through interactions within groups.

Though this section has focused on the use of a particular form of encryption, we should note that the use of this encryption constitutes just one type of digital security practice, one which is not always appropriate for a user's given situation. The use of encryption offers an incomplete form of protection and can additionally constitute a form of exposure: its use can sometimes draw attention to activists in repressive environments if they have their electronics inspected or confiscated, or if certain activities are monitored online. Additionally, the use of OTR within commercial platforms does not stop the metadata—information about who is speaking to whom, at what time—from being collected by Facebook or subsequently exposed to anyone who gains access to a user's account. We thus see that digital security practices dependent on currently available tools can only offer a piecemeal form of protection, even when implemented with careful consideration. We note that tool improvement is difficult and slow moving in an environment that favours commercial technologies, thus explaining why Free and Open Source Developers have not been able to solve the above dilemmas despite years of dedicated work to fix shortcomings.

Conclusion

The women's and LGBTQI rights network we have discussed in this article highlights the importance of social structures for privacy and digital security—with regard to both strategies and technical tools. That this network had to respond to threats in such a self-reliant way reflects a forced responsibilisation for digital technology users who want some protection of and control over their privacy and digital security. This network does highlight that building and sharing collective security strategies can contribute to the efficacy and longevity of activism, while also helping to lessen the burden of responsibility in learning to mitigate the harms of digitally mediated threats. Nonetheless, the resource differential between this network and their harassers—some of which are governmental actors—was enough that no matter what actions the activists took, they continued to face significant and unpredictable threats. Digital security strategies cannot remove all threats; they can only mitigate their effects. The strong social ties between individuals and organisations in the women's and LGBTQI rights network helped facilitate the continuation of their activism despite a multitude of threats, demonstrating a necessity for the human rights sector to brainstorm, develop, and support group-centric approaches to privacy

and digital security. We argue that since group-centric approaches to privacy and digital security can help increase overall levels of efficacy and protection, such approaches should be prioritised in the creation of strategies, policies, and tools developed by and with computer scientists, advocates, and policy makers, within the human rights sector and beyond.

Notes

[1] Anonymous #1 / Location redacted (2014). Interview with Becky Kazansky, Location Redacted, 11/2014. Unpublished transcript.

[2] Anonymous #2 / Location redacted (2014). Interview with Becky Kazansky, Location Redacted, 11/2014. Unpublished transcript.

[3] Anonymous #3 / Location redacted (2014). Interview with Becky Kazansky, Location Redacted, 11/2014. Unpublished transcript.

[4] Anonymous #4 / Location redacted (2014). Interview with Becky Kazansky, Location Redacted, 11/2014. Unpublished transcript.

[5] Anonymous #5 / Location redacted (2014). Interview with Becky Kazansky, Location Redacted, 11/2014. Unpublished transcript.

[6] Anonymous #6 / Location redacted (2014). Interview with Becky Kazansky, Location Redacted, 11/2014. Unpublished transcript.

[7] Anonymous #7 / Location redacted (2014). Interview with Becky Kazansky, Location Redacted, 11/2014. Unpublished transcript.

[8] Anonymous #8 / Location redacted (2014). Interview with Becky Kazansky, Location

Redacted, 11/2014. Unpublished transcript.

[9] Anonymous #9 / Location redacted (2014). Interview with Becky Kazansky, Location Redacted, 11/2014. Unpublished transcript.

Acknowledgements

An enormous thank you is due to the groups who shared stories highlighted in this article, as well as to various staff and friends of Tactical Tech for supporting this research and for providing critical feedback on earlier drafts.

Biographical Note

Becky Kazansky is Lead Programme Researcher at Tactical Technology Collective. Through research and facilitation, she supports the development and implementation of privacy and digital security strategies to defend and extend human rights.

References

Andrejevic, Mark. 'The Work of Watching One Another: Lateral Surveillance, Risk, and Governance,' *Surveillance & Society* 2.4 (2005): 479–497.

Ausloos, Jef. 'Guidelines for privacy-friendly default settings,' (KU Leuven, 2012): 34, https://www.cosic.esat.kuleuven.be/publications/article–2297.pdf

Balsa, Ero, Laura Brandimarte, Alessandro Acquisti, Claudia Diaz and Seda Gürses. 'Spiny CACTOS: OSN Users Attitudes and Perceptions Towards Cryptographic Access Control Tools,' *Internet Society*. USEC '14, 23, San Diego, CA, USA (2014), https://www.Internetsociety.org/sites/default/files/02_2-paper.pdf

Barnard-Wills, David and Debi Ashenden. 'Public Sector Engagement with Online Identity Management', *Identity in the Information Society* 3.3 (2010): 657–674.

Barocas, Solon, and Helen Nissenbaum. 'On Notice: The Trouble with Notice and Consent,'

Proceedings of the Engaging Data Forum (2009) http://www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf Baumer, Eric, Phil Adams, Vera D. Khovanskaya, Tony C. Liao, Madeline E. Smith, Victoria Schwanda Sosik, and Kaiton Williams. 'Limiting, Leaving, and (re)Lapsing: An Exploration of Facebook Non-Use Practices and Experiences', *CHI Changing Perspectives* (2013).

Bickert, Monica. 'Explaining Our Community Standards and Approach to Government Requests' (2015), http://newsroom.fb.com/news/2015/03/explaining-our-community-standards-and-approach-to-government-requests/

Bigo, Didier. 'Globalized-In-Security: the Field and the Ban-Opticon', in Sakai N, Solomon J (eds). *Translation, Biopolitics, Colonial Difference* (Hong Kong: University of Hong Kong Press, 2006): 109–156.

Braman, Sandra. *Change of State: Information, Policy, and Power* (Cambridge: MIT Press, 2006): 130.

Citizen Lab. 'Communities at Risk' (2014), https://targetedthreats.net/

De Wolf, Ralf, Rob Heyman, and Jo Peirson. 'Privacy by Design Through Social Requirements Analysis of Social Network Sites from a User Perspective' (2013), https://www.utwente.nl/bms/steps/research/colloquia_and_seminars/colloquia/bestanden/2013–2014/pierson2013.pdf

European Union Commission. 'Commission Decisions on the Adequacy of the Protection of Personal Data in Third Countries' (2014), http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

European Union. 'Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data,' 24 October (1995), http://ec.europa.eu/justice/policies/privacy/docs/95–46-ce/dir1995–46_part1_en.pdf

Facebook Inc. 'Community Standards' (2015a), https://www.facebook.com/communitystandards

Facebook Inc. 'Government Requests Report' (2015b), https://govtrequests.facebook.com/country/United%20States/2014-H1

Facebook Inc. Facebook Help Center. 'What are the privacy options for groups?' (2015c), https://www.facebook.com/help/220336891328465

Federal Trade Commission. 'Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises' (2011), http://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep

Garland, David. 'The Limits of the Sovereign State: Strategies of Crime Control in Contemporary Society', *The British Journal of Criminology* 36 (1996): 445–471.

Gellman, Barton and Ashkan Soltani. 'NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say', *The Washington Post,* October 30 (2013), http://

www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e–4166–11e3–8b74-d89d714ca4dd_story.html

Goldberg, Ian, Berkant Ustaoglu, Matthew D. Van Gundy and Hao Chen. 'Multi-Party Off-the-Record Messaging', *CCS'09,* 9–13 November (Chicago, IL: 2009), http://www.cypherpunks.ca/~iang/pubs/mpotr.pdf

Gürses, Seda. 'Attitudes Towards "Spiny CACTOS"' (2014), http://vous-etes-ici.net/?p=80

Hankey, Stephanie and Daniel O'Clunaigh. 'Rethinking Risk and Security of Human Rights Defenders in the Digital Age', *Journal of Human Rights Practice* 5.3 (2013): 535–547.

Hill, Kashmir, 'Facebook Added 'Research' To User Agreement 4 Months After Emotion Manipulation Study', (2014 June 30) http://www.forbes.com/sites/kashmirhill/2014/06/30/facebook-only-got-permission-to-do-research-on-users-after-emotion-manipulation-study/

Human Rights Watch. 'With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law, and American Democracy' (2014). https://www.hrw.org/reports/2014/07/28/liberty-monitor-all–0 Iyengar, Shanto. 'Framing Responsibility for Political Issues: The Case of Poverty', *Political Behavior* 12.1 *Cognition and Political Action* (1990): 19–40.

Kirkpatrick, David. *The Facebook Effect: The Inside Story of the Company That Is Connecting the World* (New York: Simon & Schuster, 2010).

Marx, Gary. 'A Tack in the Shoe and Taking off the Shoe: Neutralization and Counter-Neutralization Dynamics', (2009) http://web.mit.edu/gtmarx/www/shoe.pdf

Meyer, D. 'Facebook Prism Case Heads to Europe's Highest Court' (2014 June 18) https://gigaom.com/2014/06/18/facebook-prism-case-heads-to-europes-highest-court/

Nissenbaum, Helen. *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford Law Books, 2010).

Notley, Tanya and Stephanie Hankey. 'Human Rights Defenders and the Right to Digital Privacy and Security,' In John Lannon and Edward F. Halpin (eds). *Human Rights and Information Technologies: Trends and Consequences of Use* (Hershey, PA: IGI Global, 2013): 157–175.

Pen America. 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor', (2013) http://www.pen-international.org/read-pen-american-centres-report-chilling-effects-nsa-surveillance-drives-writers-to-self-censor/

O'Malley, Pat. 'Responsibilization', in A. Wakefield, & J. Fleming (eds). *The SAGE Dictionary of Policing* (London: SAGE, 2009), 277–279.

Ohm, Paul. 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,' *UCLA Law Review* 57.6 (2010): 1701–1777.

Schwartz, Bari. 'Hot or Not? Website Briefly Judges Looks', *The Harvard Crimson* (2003 November 4) http://www.thecrimson.com/article/2003/11/4/hot-or-not-website-briefly-judg-

es/

Shamir, Ronen. 'The Age of Responsibilization: On Market-Embedded Morality', *Economy and Society* 37.1 (2008): 1–19.

Solove. Daniel. 'A Taxonomy of Privacy', *University Of Pennsylvania Law Review* 477 (2006): 477–560.

Solove, Daniel. 'Privacy Self-Management and the Consent Dilemma,' *Harvard Law Review* 126 (2012): 1880–1903.

Stallman, Richard. 'How Much Surveillance Can Democracy Withstand?' (2013 October 14) http://www.wired.com/2013/10/a-necessary-evil-what-it-takes-for-democracy-to-survive-surveillance/

Tactical Technology Collective and Front Line Defenders. 'Security in a Box', (2015) https://securityinabox.org/en

Tactical Technology Collective and Front Line Defenders. 'Towards Holistic Security for Rights Advocates', (2014) https://tacticaltech.org/holistic-security

Tsing, Anna Lowenhaupt. *Friction: An Ethnography of Global Connections* (Princeton N.J.: Princeton University Press, 2005).