What harms may come?

Exploring the anticipatory dimensions of surveillance resistance in an age of datafication

Kazansky, B.

Publication date
2021

Chapter 4. ‘It depends on your threat model’: the anticipatory dimensions of resistance to data-driven surveillance[7]

7 This chapter has been published as a peer-reviewed research article: Kazansky, B (2021) “It depends on your threat model”: Understanding the anticipatory dimensions of resistance to datafication”. *Big Data & Society* (8)1, online first. The version of the chapter which appears here is unaltered in content, other than the removal of acknowledgements, the re-formatting of citations and footnotes, and a change in wording for how I refer to my previously published work in the texts. Where in my published articles, I refer in line to the texts as an ‘article’, these have been changed to ‘chapter’. Where I discuss my own previously published thesis chapters in these two articles through standard citation practices, in the thesis text I cite these by chapter number.

Abstract

While many forms of data-driven surveillance are now a ‘fact’ of contemporary life amidst datafication, obtaining concrete knowledge of how different institutions exploit data presents an ongoing challenge, requiring the expertise and power to untangle increasingly complex and opaque technological and institutional arrangements. The how and why of potential surveillance are thus wrapped in a form of continuously produced uncertainty. How then, do affected groups and individuals determine how to counter the threats and harms of surveillance? Responding to an interdisciplinary concern with agency amidst datafication, this chapter explores what I term ‘anticipatory data practices’ – future-oriented practices which provide a concrete anchor and a heuristic for action amidst the persistent uncertainties of life with data. This chapter traces how anticipatory data practices have emerged within civil society practices concerned with countering the harms of surveillance and data exploitation. The empirical analysis of this chapter draws from 50 interviews with digital security educators and technology developers; participant observation at 12 civil society events between 2016 and 2019 and the textual analysis of 100 security manuals produced by NGOs and grassroots groups.

Introduction

Data-driven surveillance is often made evident to its targets only following punitive measures such as arrests, campaigns of harassment and violence and discriminatory effects (Browne, 2015; Eubanks, 2018; Ullrich and Knopp, 2018). Those seeking protection from its harms must thus grapple with an unknown number of 'intrusive-unseen' threats, (Wang, 2018: 257) which loom large yet remain imperceptible until harm has been done. As Smith (2018) points out, the opacity of this dynamic is no accident. Whereas the contemporary ubiquity of known data collection, monitoring and profiling normalises the assumption that any data generated throughout daily life will be exploited towards different ends (Duffy and Chan, 2018), concrete knowledge of how exactly governments and corporations surveil and exploit data is often out kept out of reach (Gangadharan and Niklas, 2018). When the implicated arrangements of power and technology are brought to light through investigation, these arrangements shift so as to obscure the picture once more (John, 2011; Strathern, 2000). The sites, techniques and rationales of data monitoring and exploitation are thus wrapped within a continuously produced uncertainty. How then, do affected groups and individuals determine how to counter the threats and harms of surveillance?

Challenging the idea that people have succumbed to 'digital resignation' (Draper and Turow, 2019), a multitude of potential tactics are marshalled to cope with the 'mess' of data and digital life (Pink et al., 2018) and counter 'imagined surveillance' (Duffy and Chan, 2018). People disclose information selectively to certain parties (Marwick and boyd, 2014);'back up', guard and duplicate important information (Pink et al., 2018); engage in 'vernacular resistance' through obfuscation (Brunton and Nissenbaum, 2015) and create new technologies to shield against tracking and profiling (Kazansky and Milan, Forthcoming; Milan and Van der Velden, 2016). For targeted groups and populations, the high stakes of surveillance

'discovery' (Marx, 2009) has resulted in a continuous adaptation of practice (Kaun and Treré, 2018). Techniques of resistance must stay abreast of techniques of surveillance (Leistert, 2012). However, despite their constant adaptation, resistant tactics and strategies do not necessarily succeed in their goals (cf. Brunton and Nissenbaum, 2015). As Hong (2015) points out, amidst the unknowns of surveillance, counter-measures might instead only provide a 'simulation of safety'(70). How exactly to act and adapt – in other words, which tactics and strategies will bring desired effects in unstable and contingent situations – is thus subject to continuous controversy (Musiani and Ermoshina, 2017). The question of what constitutes an 'effective' tactic to resist surveillance and counter data harms is one of ongoing inquiry both in academic literatures and across social movements (Aouragh et al., 2015; Dencik et al., 2016; Gürses et al., 2016; Monahan, 2006).

Responding to an interdisciplinary imperative to deepen understandings of resistance and agency amidst datafication (Couldry and Powell, 2014; Kennedy et al., 2015), this chapter explores two related practices enacted by affected communities to fight digital resignation and facilitate agency: 'threat modelling' and 'risk assessment'. These interrelated practices sit within a larger cluster of what I term 'anticipatory data practices'. Concerned with determining the likelihood of imagined potential surveillance-related harms, anticipatory data practices take up the task of untangling data 'mess' and 'cobbling what we know and suspect into a picture of a sensible, working world' (Hong, 2015: 73). Through structured, future-oriented modes of sensemaking, they serve to tame the uncertainties of contemporary surveillance, turning political strife and unpredictable danger into a 'manageable' problem. In recent years, several scholars have highlighted the prevalence of practices such as threat modelling and risk assessment amongst technologists and activists concerned with digital security and surveillance counter-measures. Ermoshina and Musiani (2018) characterise threat modelling and risk assessment as 'powerful instruments to narrow down and structure'

interventions intended to bolster security and safety for activists (p. 32). Myers West (2017) highlights the 'extensive time and energy' spent by civil society groups 'building threat models, and calibrating their activities in response'. Through a multi-year study, this chapter delves deeper into these important practices, exploring how their 'anticipatory logics' (Anderson, 2007, 2010) enable digital security specialists and civil society groups to cope with surveillance-related uncertainties. The chapter also interrogates the political commitments these practices create through their focus on future-oriented modes of action. In so doing, the chapter brings into dialogue contemporary literatures on anticipation with studies of activism, resistance and data practices, aiming to advance a critical perspective on resistance and agency in times of datafication.

The plan of the chapter is as follows: I first contextualise the notion of anticipation in relation to data practices and surveillance resistance, building up my notion of 'anticipatory data practice'. Following, I explain the methodology of my study. Next, I provide context on the state of civil society practices to counter-surveillance, examining the sectoral shifts which have created an imperative to apply anticipatory data practices. I situate the growing importance of anticipatory data practices in relation to a disillusionment within civil society over the past years with the 'digital universalism' (Chan, 2013) and 'design from nowhere' (Aouragh et al., 2015: 226) which have characterised tech-centric 'solutions' to surveillance risks. As practices which grapple with uncertainty and situational contingency, I argue that anticipatory data practices can be understood as an attempt to break from totalised conceptualisations of surveillance and generic 'solutions' to its harms. Yet, I also argue that civil society's turn to 'anticipatory modes' of response to surveillance requires a critical lens due to the totalising and hegemonic status of anticipatory regimes in contemporary life (Adams et al., 2009). Hence, this chapter ends with a critical analysis of the forms of agency facilitated through practices which harness anticipatory logics.

Situating anticipation

Anticipation can be understood as the future-oriented dimension of action, the 'process through which the present is transformed, intervened in and ultimately governed in the name of the future' (Alvial-Palavicino, 2015: 137). As Adams et al. (2009) point out, anticipation has 'multiple valences' (p. 247); affective, political, temporal and material. Risk, speculation, prediction, preemption and prevention can be understood as conceptually interlinked, if distinct 'anticipatory logics' (Anderson, 2007, 2010). The interdisciplinary study of anticipation thus draws necessarily on a vast genealogy of literature, building on studies of risk (Beck, 1992; Jasanoff, 1998) histories of finance and actuarial practices (Bouk, 2015; Hacking, 1975), national security and counterterrorism (Amoore, 2013; Aradau and Blanke, 2017; De Goede, 2012) and data-driven surveillance (Brayne, 2017; Dencik et al., 2018; Lyon, 2014; Van Brakel, 2016). The task of tracing and articulating overlaps and disjunctures in anticipatory logics forms a central locus of scholarly analysis. For example, in studies of policing and national security, what designates an anticipatory action as 'preemptive' rather than 'preventive' is explored as a crucial yet tricky ontological distinction contingent on the political justification for violent state intervention in advance of anticipated harmful events (Andrejevic, 2017; Massumi, 2015). Meanwhile, critical studies of state and corporate security practices highlight the 'mobility' of anticipatory logics and practices from one realm of action to another amidst the continued reverberations of exceptional events such as the terrorist attacks of 11 September 2001 (Amoore, 2013; O'Grady, 2016). Studying the preemptive logics of data-driven policing in the United States, Miller (2019) warns that a disciplinary preoccupation with the post-'9/11' world can obscure longer histories of social control as they come to bear on contemporary anticipatory regimes, honing in on the roots of predictive policing in anti-Blackness and white supremacy.

The tricky ontological distinctions, 'mobile' practices and complex histories of anticipatory logics and practices clearly demand an attunement to the situationally specific ways they arise. As I will highlight later, the practices that form the focus of this chapter appropriate a number of conventions from different realms of anticipatory action yet are reconfigured to fit the values of civil society actors and their surveillance-resistant practices. Thus, one goal of this chapter is to trace how anticipatory practices and their logics are transformed as they are re-appropriated in the context of civil society work, building on an understanding of practices as stabilised yet situationally specific entities (cf. Shove et al., 2012; Star and Griesemer, 1989). It is important to highlight that in the literatures mentioned earlier, anticipation is predominantly configured as an element of state and corporate regimes. The question, then, is how to study anticipatory logics and practices as they arise amongst civil society actors, who operate beyond state and corporate arenas. One clue comes from literature engaging with everyday data practices. Whereas studies of state and corporate action often highlight how anticipatory logics arise in 'exceptional' circumstances such as national security or disaster management, studies of everyday data practices situate anticipation as a banal element of technological use. Pink et al. (2018) argue that 'anticipatory modes' are in fact intrinsic to coping with the 'mess' of data, with uncertainty (and the subsequent draw to anticipate) always at play. The authors highlight the implicitly anticipatory dimensions of practices such as saving or 'backing up' data digitally, arguing that 'saving data indicates that data needs to exist in an as-yet-unknown but imagined future' (p. 10). Similar to the act of saving data, practices around self-disclosure on social media are seen by Marwick and boyd (2014) to rely on an 'envisioned boundary' (p. 1058) of how this information might be used by different parties – something that becomes difficult to anticipate amidst online 'context collapse'. Within 'data relations' (Kennedy, 2016), the configuration of practice can thus be understood as folding around the question of how an action taken at present might be valuated and subsequently exploited in the future.

Implicit ‘anticipatory modes’ are also evident in theoretical works on the interactional dynamics of surveillance resistance. In conceptualising the ‘moves’ and ‘counter-moves’ that unfold in the interactions of those surveilling and surveilled, Marx (2009) observes an ‘adversarial social dance’ (p. 299), which is ‘part of a dynamic system that includes and anticipates the behaviour of agents’, implying that anticipation is intrinsic to the agency of both the surveilling and surveilled (Marx, 2016: 168). Marx (2016) offers a concrete example in ‘security consultants’ who ‘advise clients with sensitive information not to use an unsecured telephone, fax, or Internet connection unless they would not mind seeing their communications in the newspaper the next day’ (p. 150). Bridging studies of data practices and surveillance dynamics, anticipation can thus be understood as an implicit dimension of data practices as well as a thread which ties the interactional dynamic of the so-called ‘dance of surveillance’ together. Yet, as I will show, the anticipatory data practices of focus in this chapter play a distinct role in relation to the broader milieu of implicitly anticipatory practices (such as the backing up of data or use of encryption tools) highlighted by Pink et al. (2018). In contrast to the practices which they highlight, I argue that risk assessment and threat modelling practices are explicitly anticipatory, meaning that they are formally structured around the central goal of threat anticipation. Furthermore, as explicitly anticipatory practices, they serve as ‘triggers’ for ‘other future-oriented activities’, per Alvial-Palavicino’s (2015: 154) conceptualisation of anticipatory practices. In this chapter, I will show how anticipatory data practices – threat modelling and risk assessment in particular – trigger further anticipatory action by guiding people towards the use of particular technological ‘tools’ which counter-surveillance and data ‘mess’.

Methods

The analysis in this chapter draws from a multi-sited study of civil society responses to the shifting threats of digital surveillance and datafication. The study was comprised of 50 semi-structured interviews with technologists, educators and targeted communities; participant observation at 12 digital rights and Internet freedom meetings between 2015 and 2019 and from a discursive analysis of 100 published manuals on security, privacy and surveillance self-defence. Documents analysed included activist training manuals, technical literatures on threat modelling and digital literacy and 'awareness' texts. The focus of analysis was put on strategies and tactics for anticipating threats and harms, with attention paid to the way different texts construct notions of risk, threats and anticipatory logics. Participant observation was conducted in two types of civil society events: international meetings bringing together dispersed networks of individuals and groups to showcase new projects, discuss best practices and set priorities and agendas for future collaborations and small, closed workshops organised to develop specialised tactics and strategies of defence from surveillance.

Interviewees were based in a total of 26 countries from across different regions of the world. Their diffuse geographical representation resulted from the transnational patterns of coordination common for civil society projects concerned with digital issues such as Internet freedom, counter-surveillance and digital rights (Myers West, 2017). A number of interviews were conducted at the site of their international meeting points. Interviewees were selected for their contributions to counter-surveillance practices as educators, technologists and representatives of surveillance-affected communities. They were asked to reflect on the changing state of their field and to describe the tactics and strategies they use to identify and counter 'digital' threats. Names and identifying details – including specific organisations, countries and in many cases regions – have been

anonymised to respect the sensitive nature of the work documented in this study. Of note, the analysis in this chapter gives outsize space to the perspectives of educators. Fitting under the educator category are people identifying as facilitators and digital security trainers, whose role is to work with affected communities to 'raise awareness' of digital surveillance threats, increase technological literacy and promote particular counter-measures (Ermoshina and Musiani, 2018; Kazansky, 2015).

The choice to focus on educator perspectives is due to their observed role in 'translating' (see: Star and Griesemer, 1989) the viewpoints and methodologies of defensive counter-surveillance practices between technologists and surveillance-affected communities. Their positioning between communities of practice provides a way to trace the varied configurations and re-configurations of practice which occur between social worlds. Building directly on lexicon common to civil society actors interviewed, 'translation' in this chapter also refers to their widely professed aim to form an accountable line of communication between technology-focussed actors and affected communities. Educators work to make 'technical' concepts legible beyond specialist niches, with the aim to 'spread awareness' of potential technological harms. Going the other way, educators collect and synthesise accounts of technologically related problems faced by affected communities, framing them in terms familiar to technologists in the hopes that they will better shape technological design processes to meet affected community 'needs'. As with any translation, the process is not a neutral one, serving to highlight frictions and differences amongst the social fractals that together make up what Price (2003) terms 'transnational civil society'. I will further argue that the educators' role of translating and promoting anticipatory data practices is endowed with a form of productive power and expertise which causes them serve as 'agents of anticipation' (cf. Mackenzie, 2013) – enrolled and enrolling others into anticipatory modes of work. Thus, the perspectives and activities of educators offer two forms of insight: first, a path to understanding agency as it manifests in a particular data practice

and second, a way to trace the emergence of the imperative to anticipate threats.

Digital security and digital universalism: Friction and critique

For several decades, transnational civil society actors have worked to intervene in digital technologies and their consequences for society (Hintz and Milan, 2013, McInerney, 2009). In the wake of what become known as the 'Arab Spring', issues around 'information controls' and digital surveillance became a growing locus of concern (Citizen Lab, 2014; Hankey and O'Clunaigh, 2013), which reached a peak in public interest directly following the Snowden leaks in 2013 (Dencik and Cable, 2017; Milan and Van der Velden, 2016). Amidst these developments, the work of civil society actors concerned with digital surveillance has converged around an internationally dispersed 'digital security ecosystem' (the Engine Room, 2018) This 'ecosystem' of organisations and groups coordinates and formalises mechanisms of defence from a shifting milieu of threats. 'Digital security', as scoped by interviewees, encompasses a wide breadth of tactics and strategies to prevent or mitigate harms resulting from targeted digital intrusion, 'mass' government surveillance, corporate privacy violations and data-driven profiling. Privacy-enhancing technologies have been developed to preserve 'online' anonymity, secure, obfuscate data and gain access to censored information (Brunton and Nissenbaum, 2015; Musiani and Ermoshina, 2017; Rogers and Eden, 2017). Digital security trainings are organised to teach tools and tactics of response (Daskal, 2018; Ermoshina and Musiani, 2018; Kazansky, 2015) and improvements are made to the technical infrastructures of organisations and emergency support is proffered in the wake of digital attacks (Citizen Lab, 2014). Altogether, these advancements present the

picture of a maturing ‘field’ with increasingly specialised forms of expertise and formalised protocols (the Engine Room, 2018).

Yet these advancements have also produced social frictions (Costanza-Chock et al., 2018). Aouragh et al. (2015) argue that the labour divisions and politics of expertise bound up in the development and promotion of digital surveillance counter-measures have resulted in ‘sneaky moments’ that reinstate the very hierarchies and structures being fought against. In their analysis of civil society campaigns promoting digitally secure practices, they critique the ‘tendency for tech activists to develop universal technologies with a ‘design from nowhere” (p. 226), which are then positioned as solutions to complex social problems. This ‘design from nowhere’ parallels the ‘digital universalism’ which Chan (2013) finds embedded into dominant discourses and practices of technological development. Educators interviewed for this study critique a resulting expectation that affected communities adopt the use of potentially inappropriate, ‘tool-centric solutions’ (Interview #43). ‘Every technologist you ask, they say, you wanna be secure, just use Tor, use Signal’, joked a digital security trainer referencing the prevalent recommendation in the ‘digital security community’ that those concerned with the confidentiality of their data use these two particularly robust software tools for safer communications (Interview #14). As the trainer pointed out, the use of these tools can in fact increase the vulnerabilities their developers claim to counter. For example, at the time of writing, the Signal chat application requires the disclosure of a personal phone number in order to set up a ‘user account’, data which may expose a person to further surveillance (Shelton, 2018). A number of interviewed trainers and human rights defenders (HRDs) noted in our discussions that Tor, a tool widely used to circumvent censorship, has often ‘failed’ to work for a number of reasons, ranging from efforts by governments to block the tool’s use, to the slow Internet speeds still found across many rural regions of the world. Thus, ‘at best, these approaches typically build skills for particular tools without an ability to adapt’, notes Norman Shamas, an educator proposing to

discuss how to ‘create a pedagogy of empowerment’ at a large annual meeting bringing together the international Internet freedom community (Shamas, 2017). With safety a concern, the 2019 edition of the same conference included a workshop by staff of the Electronic Frontier Foundation (EFF) asking ‘How Can We Share Secure Messaging AdviceWithout Causing Harm?’ The session description notes ‘the best choice for one person could be catastrophic for another’ (Li and Trendacosta, 2019).

The problems of ‘tool-centric solutions’ were seen by my interviewees to be directly related to an increasingly critiqued ‘white northern male-dominated expert culture’ on matters of digital security (Interview #35). Funding sources and support infrastructures remain concentrated within homogenous North American and Western European institutions, at the same time that interventions have predominately been directed towards supporting ‘front-line’ groups across the so-called ‘global south’ (Brooks, 2019). The result is a style of support that has experts who ‘lack context’ and ‘parachute in from somewhere else’ to provide ‘one-off’ interventions (Interview #5). According to digital security trainers who have long fought to reform civil society’s approaches to education and technological development, the universalism inherent to this ‘parachute model’ has, rather than simplifying life amidst data mess and exploitation, contributed to a mounting pressure for those affected by surveillance ‘to know everything’ about matters of digital surveillance (Interview #8). An advocate working with HRDs across Central America explained that amidst ‘too many things happening’ she finds herself and the groups she works with torn between tasks, from continuously scanning the horizon for new information control laws, surveillance technologies and politically oppressive measures; to at the same time trying to mitigate persistent troubles stemming from a basic lack of resources (Interview # 41). ‘Being aware of what big events are happening, adapting to them and making that part of your security workflow’ (Interview #7) is understood as a

requirement, yet is ‘like living with a gun under your bed’ (Interview #8), added two other interviewed digital security trainers.

The need to monitor emerging threats amidst the constraints of persistent troubles means, according to a digital security trainer working with HRDs under ‘direct threat’ of authoritarian regimes, that ‘people get overwhelmed and can instead ‘end up doing nothing’, which has in turn opened up groups to ‘really critical and existential’ vulnerabilities (Interview # 42). Thus, a digital security trainer who has worked with front-line human rights groups for 20 years questioned what he observes as a continuously increasing duty to monitor the advancement of every concerning new digital technology and its potential harms. In a discussion around the manifold ‘physical’ security issues faced by a coalition of persecuted land rights defenders in a rural area with little digital infrastructure, he wondered ‘is it really a useful form of awareness…to know that there are now smart facial surveillance cameras “everywhere”?’ (Interview #9). The globalised ‘everywhere’ in this case referred to someplace else. Reflecting with ambivalence on his role as someone charged with spreading awareness of threats, another digital security trainer argued that ‘people must know it is happening…but shouldn’t be scared or paranoid’ (Interview #8). How to determine what is indeed worth worrying about is thus a central aim of educators aiming to show that effective surveillance counter-measures are possible in spite of the aforementioned troubles.

From the universal to the contingent: Enter threat modelling

Amidst the growing disenchantment with universalised interventions to complex problems, interviewed technologists and educators were quick in

interviews to answer that what should be done in response to the many potential worries over digital surveillance and related 'digital threats' 'depends on your threat model'. The term 'threat model', aside from serving as a ubiquitous conversational anchor, refers to a number of variable exercises enacted within digital security trainings and within the 'workflows' of technical experts. Interviewees describe threat modelling as a way to anchor thinking amidst an overwhelming sense of globalised risk. The task, as one digital security trainer puts it, is to 'break (uncertainty) down into logical boxes' (Interview #42). Through the enactment of threat modelling exercises, the unknowns of surveillance are first tamed into thinkable threats, defined as a set of finite contingencies and finally mapped to tactical counter-measures deemed effective to the particular situation at hand, 'helping people make the best decision with the tools that are available' (Interview #6). Threat modelling might, for example, make clearer which encrypted chat tool or Internet service provider would best preserve privacy for a person accessing the Internet from a particular digital device, at a particular place and time. The threat model thus serves to establish a heuristic for tactical action. One widely promoted threat modelling exercise can be found in the Surveillance Surveillance Self-Defense Guide (SSD) by the Electronic Frontier Foundation (EFF). This guide defines threat modelling as 'a way of narrowly thinking about the sorts of protection you want for your data' (Electronic Frontier Foundation, year unknown). A series of questions guide the reader to narrow a confusing calculus to a smaller spectrum of objects and scenarios to consider:

> What do you want to protect? Who do you want to protect it from? How likely is it that you will need to protect it? How bad are the consequences if you fail? How much trouble are you willing to go through in order to try to prevent those? (Electronic Frontier Foundation, year unknown)

When asked how threat modelling became such a prevalent point of reference within civil society, several interviewed digital security trainers recalled first hearing about the practice in 2012, amidst a spurt of new collaborations aiming to match the expertise of tech industry-employed engineers and technologists to the needs of under-resourced non-profit civil society organisations. In the fields of software and security engineering, numerous methodologies of threat modelling had been developed since the 1990s as a process for building security features into information infrastructures (Galvez and Gürses, 2018). In these specialist fields, threat modelling processes were introduced into engineering teams to help mitigate against an ever-growing milieu of potential 'attack scenarios' against information systems. The author of a highly referenced book on threat modelling explains that the practice allows security actors to take a proactive, anticipatory approach to security; to 'find design issues before you've even written a line of code' rather than wait for security problems to occur and then try to 'patch' them one by one after an attack (Shostack, 2014: xxiii).

Per interviewed digital security trainers, threat modelling was introduced by technologists into civil society as an aid to help non-profits structure and prioritise their own growing concerns with information management and digital vulnerabilities. However, a translation of practice was required in order to make threat modelling a meaningful practice beyond a specialist niche. One digital security trainer explained that 'technology developers learn how to model the perfect technical system…but not how to make compromises' (Interview #12). This lamented lack of 'compromise' harkens back to long-running debates in computer science around the tendency of technology developers to 'configure the user' (Woolgar, 1990) around the affordances of systems already built, rather than shape the engineering process around their complex needs.

In the form of threat modelling promoted by digital rights organisations such as the EFF, an effort is made to refit the practice around the vantage

of a motivated individual ‘user’ rather than an optimal system or ‘technical’ team of engineers. Yet some artefacts of its engineering origins remain: as Aouragh et al. (2015) point out, the technical terminology of threat modelling, as envisioned by the EFF, flattens the complexities of life into ‘assets’, asking the readers of its guide to think about who might want to do harm to them. ‘Assets’ – a term common to both finance and computer security – come to stand in as the unit for understanding the value of things, people or ideas that might be under threat. In effect, the guide’s ‘users’ are asked to reimagine their life as an asset management system with inputs and outputs. The ‘output’ of threat modelling, per the guide, is a selection of digital security tools from which the user can choose a counter-measure designated as appropriate for the constructed threat model. The simplification achieved through this form of threat modelling is what Clarke (2015) argues is a central function of anticipatory logics.

Assessing risk: Situational awareness versus self-care

Alongside threat modelling, interviewed educators also turn to the closely related practice of ‘risk assessment’ to surface, map and mitigate the concerns of affected communities worked with. Although the burgeoning field of ‘risk assessment’ methodologies has well-documented roots in insurance and financial speculation (Bouk, 2015; Hacking, 1975), the focus in this chapter is on understanding the configuration of risk assessment as it arises in digital security trainings and organisational digital security processes particular to civil society. As I will show, some conventions and discourses persist while morphing to account for the values and goals particular to civil society. A security guide titled the Front Line Defenders (2011) Workbook on Security offers a conceptual

window onto risk assessment particular to civil society, featuring several chapters devoted to different elements of assessing risk for an intended audience of 'high-risk' HRDs. One section in particular focuses on behavioural strategies where surveillance is suspected. Here, the anticipatory elements of the practice are made explicit, with a pedagogical focus built around the assumption that surveillance is more likely than not. 'Make a plan for how you would deal with this before it happens to you', the workbook directs (p. 36). It advises that HRDs who suspect they might be under surveillance should 'assume that you are' (p. 39). Furthermore, it recommends that HRDs 'make a list of the actions you will take to deal with the situation' (p. 37) though it also emphasises that 'it is important to maintain a balance between taking precautions and not becoming paranoid' (p. 36). As such, the workbook reflects a fundamental ambivalence towards the notion of 'awareness' and vigilance, demonstrating also a sense of resignation to the idea that surveillance is unavoidable.

In my analysis of security guides, observations of digital security trainings and interviews with educators, the notion of risk assessment is commonly conflated or improvisationally combined with threat modelling exercises. The main goal is the same: to map a 'mess' of concerns to 'solutions' of different forms. There are, however, several differences in how the goals of these practices are presented. Whereas threat modelling is commonly framed around the goal of attaining or maintaining security, risk assessment, as articulated by interviewees, focuses on goals and outcomes other than security itself. One digital security trainer working with peace-building groups in post-conflict regions explained that 'the risk assessment process for the community we are working on starts with asking people about who they are, about why they are doing the work that they are doing' (Interview #5), echoing the discourse of 'outcome mapping' methodologies used in policy making and development work (Earl et al., 2001). The digital security trainer argued that an approach that centres values and motivations other than security itself shows more

solidarity with the goals of movements and is thus more 'effective'. Following this methodology, a 'security strategy' is developed by working backwards from the idealistic aims and values guiding the civil society work at hand, rather than automatically overlaying a 'negative', threat-centred security frame, as explained by another digital security trainer with a similar approach:

> I am asking them to envision the place where they want to get to, what gets them there, and what maximises their resources throughout their journey…if I do this then good things will happen, as opposed to if I don't do this bad things will happen. (Interview #11)

A second difference between how threat modelling and risk assessment are framed in civil society texts and exercises is that instead of only focussing on 'things' or 'assets' that need protection, risk assessment also emphasises the 'capabilities' of civil society actors, which, according to one digital security trainer, enables affected communities to see that despite threats and anxieties, they possess agency and power. The relationship between these units of analysis is made plain in a frequently discussed instrument used within the process of risk assessment: a 'risk equation'. As laid out in a security guide titled the New Protection Manual (Fernandez and Caraj, 2009) by human rights organisation Protection International, the risk equation requires its implementer to identify which people, objects and institutions in their life represent an 'asset', 'capacity' or 'vulnerability'. These three categories of people, objects and institutions are then commensurated in order to achieve a measure of risk, where 'risk = threats × vulnerabilities/capacities'. The process of valuation may produce a numerical figure representing the 'level' of risk at hand, which is then mapped to a set of potential actions meant to mitigate the risk. In other cases, the notion of 'risk' remains qualitative. The question of whether to apply quantifying or 'numbering' methodologies within risk assessment was a sticking point for the digital security trainers

interviewed. Some frameworks of civil society risk assessment disavow the quantitative valuation of lived experience. One interviewed digital security trainer believed quantification to be alienating, questioning, 'how do you not get lost in the formula?' (Interview #15). A second trainer similarly argued that 'using statistics on a single person is not intuitive' (Interview #10). Yet others interviewed believe numbers bring an essential feeling of tangibility to a situation that can otherwise remain in the abstract: 'Having numbers or figures or scales as to how dangerous or not dangerous stuff is heightens the sense of importance' (Interview #6). This proponent of calculative techniques acknowledges that though quantitative analysis 'can be a source of stress' it 'really pushes the change that you need'.

The risk equation featured in the New Protection Manual provides an example of the way anticipatory logics and practices travel and transform across social worlds, with educators importing anticipatory conventions from other sectors concerned with risk and threat management, and enrolling those they work with into their logics in order to 'push' 'needed' changes to the practices of affected communities. As already mentioned in the section on threat modelling practices, it is possible to trace how educators themselves are enrolled into anticipatory logics. Whereas threat modelling practices were said to be brought into civil society through collaboration with engineers, digital security trainers describe a different origin for their risk assessment methodologies. In interviews, several digital security trainers noted that the risk management protocols followed by their organisations were first established by former military personnel who had served as private contractors in conflict zones, before moving into civil society communities concerned with digital rights and Internet freedom. In the humanitarian field, risk management has been a highly institutionalised process going back to the 1990s (Duffield, 2010). While the predominant focus of risk assessments in the humanitarian field was traditionally on the physical and 'operational' dimensions of security in conflict zones, as digital technologies have became pervasive, digital

information management has become an increasingly important component of a broader risk management strategy. The pre-eminence of digital concerns created an imperative to merge multiple streams of security work into one, a project which has since 2011 been carried forward by a community of digital security trainers working with HRDs and digital rights activists to develop a 'Holistic Security' methodology (Tactical Technology Collective, 2016).

The Holistic Security methodology, however, distances itself from the militaristic undertones of humanitarian risk assessment. While the methodology makes the integration of digital, physical and 'psychosocial' elements of security its' explicit goal, it also re-frames security away from a 'deterministic or machine-centred approach' (Interview #7) to one revolving around a radical notion of 'self-care' (Tactical Technology Collective, 2016: 10), citing civil rights activist and poet Audre Lorde for inspiration. Rather than striving for an all-encompassing, militaristic 'situational awareness' (Suchman 2015), the locus of analysis is placed in the somatic experience of security and insecurity, in accordance with a professedly feminist emphasis on embodiment. While this shift entails a translation of practice similar to the EFF's refitting of threat modelling, the Holistic methodology stands in contrast to EFF's methodology in the focussed de-securitisation of language used in its guides and trainings.

As a further step in their feminist re-orientation of security, Holistic proponents set forth a care-oriented definition of security as 'wellbeing in action' (Tactical Technology Collective, 2016: 21). Care, in this context, means to reject fear of abstract threats and to instead embrace what is immanent and felt. Through its distancing from totalising conceptualisations of surveillance, the methodology tempers the militaristic compulsion to continuously engage in vigilant threat identification processes. However, the methodology still demands vigilance, to a degree. For example, as part of a process of 'Holistic risk assessment', the Holistic Security Manual requests that the individual

engage in the continued, daily analysis of potentially concerning security events in order to gain an 'accurate picture' of security (p. 59). The strong suggestion that individuals maintain awareness of potential threats, together with a rationalist focus on accuracy, demands that affected communities engage in an intensive form of anticipatory labour. This labour risks reproducing the very overwhelm which the methodology tries to mitigate (cf. Harvey et al., 2012).

From digital security to data politics: Consequences and conclusions

As concerns with surveillance and datafication have increasingly shaped the work of transnational civil society, civil society has turned to practices which aim to structure and tame the 'mess' of data. As this chapter has shown, anticipatory data practices such as threat modelling and risk assessment serve to guide action amidst the uncertainties of surveillance and data exploitation, weighing the likelihood of imagined potential future data harms, articulating situational contingencies and mapping these contingencies to appropriate counter-actions. Anticipatory data practices thus function as a heuristic aid for choosing other practices and 'tools' to counter concerns over surveillance and datafication. This process of heuristic-making takes place through the structured operationalisation of anticipatory logics. Importantly, this chapter has shown that in spreading and promoting anticipatory data practices, technologists and educators enrol surveillance-affected communities into anticipatory modes of doing and being, demonstrating the way that anticipatory orientations towards the future spread throughout civil society practices concerned with safety and counter-surveillance. My findings further show that a diverse array of conventions, practices and values are imbricated within anticipatory data

practices, strengthening the assertions by Pink et al. (2018) that 'there is no single template, logic or set of principles that is universally followed' for coping with the 'mess' of data (p. 12). Yet, while the lack of universal 'solutions' to the mess of data and digital life is certainly also a central theme here, this chapter shows that anticipatory data practices are emblematic of the urgent labour by civil society actors to bring structure to the 'mess'. In other words, the idea that how to respond to surveillance and datafication 'depends on your threat model' can be understood as an attempt to find an anchor amidst the overwhelm of contemporary data mess. Hence, the value of threat modelling and risk assessment practices is in the clarity and simplification they can provide.

The simplifying function of anticipatory data practices, however, raises critical concerns. As Aouragh et al. (2015) argue, 'directly mapping existing technological solutions onto supposed real-life experiences' (p. 209) can narrow the political imaginaries of activism. Similarly, Massumi (2015) argues that the anticipatory logic of preemption in particular, serves to close off the 'space' for politics, due to the vigilant, pre-conditioned responses that are instilled through the imperative to act in the present on the basis of the unknown futures. Per Anderson (2010), it thus makes sense to ask, 'what political and ethical consequences follow from acting in the present on the basis of the future?' (p. 778); or, as Mackenzie (2013) asks, what is the potential 'cost of learning to anticipate' (p. 393)?

In response to these critical questions, it is important to highlight that the preoccupation with practical fixes and 'anticipatory modes' of action within civil society is not uncritical or naive. First, many interviewees acknowledge that no matter how robust a privacy-enhancing technology or digital security tool, there is no single solution for 'defence' amidst the many worries that come with contemporary modes of surveillance. 'Datafication is the kind of thing that you can't solve with security tools' one activist digital security tool developer admitted (Interview #26). Furthermore, interviewees describe a growing focus on connecting work

on daily tactics with broader social critiques and issues of 'data politics' (c.f Ruppert and Bigo, 2017). An interviewed digital security trainer from a group supporting 'self-defence' in European labour unions reflected on the fact that while the work of the group began with promoting a set of particular set of digital security tools, their work has gradually shifted towards the political interrogation of datafication:

> We started with these security things having in mind that by 'digital self defence' we could at least ensure that people who are interested in privacy can really protect themselves. But we have seen the rise of massive data collection and we interpret this as a technological offence, against not only privacy but against autonomy and in a larger sense. Our digital self defence is necessary but definitely not sufficient. (Interview #17)

Another interviewed digital security trainer interviewed echoed concerns around the limits of self-defence, describing a feeling of futility in teaching people piecemeal counter-measures amidst a broader normalisation of surveillance and datafication:

> There's this corporatisation of data, which you know it's a big tsunami against which we are swimming. I don't want to say this is the end of our work, but it feels a little bit like this, because if everything can spy on us, everywhere around the world, then how do we deal with this? (Interview #11)

While his remark seems to signal a sense of resignation (per Draper and Turow, 2019), the trainer plans to continue his quest for practical counter-measures out of a belief that new footholds for resistance and agency are always emergent. Building on this belief, another digital security trainer argued that while self-defence might be a limiting frame for political mobilisation, 'for people who are in danger…that danger can't wait for

you to impact public policy' (Interview # 41). He thus further emphasises that practical fixes and daily tactics have a role to play in broader strategies aimed at achieving structural changes. Meanwhile, his concern with everyday safety highlights that the 'digital security ecosystem' (the Engine Room, 2018) of civil society is engaged not just in 'acts of symbolic resistance' (per Monahan, 2006: 516) but is fundamentally concerned with the daily survival of civil society and social movements more broadly.

To conclude, anticipatory data practices sit uncomfortably between a desire for a better world and an imperative to 'manage' the harms of our currently unjust one. As such, these practices can narrow politics and create problematic new commitments while also enabling important forms of action. Critical concerns with the productive effects of anticipation are ultimately tempered by the lived reality that 'you never know what hits you till it hits you' according to one veteran digital security trainer interviewed. 'There's still an element of the unknown at the end of the day' which 'flies in the face of all of our attempts to do risk assessment', he concludes (Interview # 37). This 'unknown' may harbour danger, but, as another interviewee emphasised, also offers hopeful possibilities. As transnational civil society moves towards more structured and coordinated modes of response to the shifting threats of digital surveillance and datafication, how it imbricates anticipatory modes of action within its practices presents an important subject for further study.