What harms may come?

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

Kazansky, B.

Publication date
2021

CHAPTER 9: CONCLUSIONS

Overview of thesis

My thesis has explored how resistance to surveillance takes shape amidst the uncertainties and harms of a datafying society. This concluding chapter has two goals: first, it summarizes the main empirical and theoretical contributions of my thesis, and second, it reflects on the broader societal questions that the thesis engages with. In the following sections of this conclusions chapter, I summarize my main research questions, before going through my research findings chapter by chapter. Following that, I summarize its theoretical and empirical contributions. Finally, I step back to reflect on my thesis findings vis-a-vis my past, present, and future work, addressing issues relating to technology, society, and the possibility to resist contemporary surveillance.

The primary question guiding my thesis was: **how does transnational civil society grapple with the uncertainties of contemporary surveillance-related threats and harms?** My objective was to understand how an ecology of transnationally coordinating technologists, security specialists, human rights defenders, and social justice community organizers negotiate the fight for human rights and social justice amidst the 'intrusive-unseen' (Wang, 2018: 257) uncertainties of contemporary surveillance and related digital threats. My broader goal in exploring this question was to explore how resistance to surveillance and its harms takes shape in a datafying society.

Throughout the five chapters that comprise the core of this thesis, I have investigated collaborations and contestations that occur between non-profit organizations, community organizers, security specialists, and technical service providers working together to

counter the threats and tame the uncertainties of surveillance in an era of datafication. This research has been ethnographic and multi-sited, drawing on participant observation of conferences, meetings, workshops, and trainings; semi-structured interviews of digital security educators, technology specialists, human rights defenders and community organizers; and archival and 'grey literature' texts related to digital and cyber security, self-defense, and counter surveillance. I have explored the interrelations between actors – as well as their practices and infrastructures – through the construction of 'institutional ecologies' (c.f. Star and Griesemer, 1989). This approach is sensitized to the differences between and productive frictions among groups with varying degrees of institutionalization; epistemologies of data, security and safety; resource differentials; and political commitments. In exploring civil society's responses to surveillance threats, I have also attended to its endemic controversies around the gendered dimensions of security and safety; the intersections of racial injustice and digital rights; diversity; and the neocolonial configurations of civil society institutions. I have connected these issues to an increasing focus on coordinated, institutionalized, and anticipatory responses to surveillance and digital threats.

The anticipatory dimensions of resistance to surveillance emerged as a central theme in my analysis. I showed that making sense of the threats of surveillance and datafication involves future-oriented, anticipatory practices, which help transform unwieldy surveillance uncertainties into manageable contingencies. These anticipatory practices emerge from a widely expressed imperative to proactively avoid or mitigate the harms of undesirable futures. I thus used anticipation as an analytic through which to understand the temporal, affective, and political dimensions of living with and contesting a

wide variety of potential threats. In my exploration of the practices and infrastructures particular to civil society's responses to surveillance, I have looked at how, to defend against surveillance threats, civil society actors appropriate anticipatory logics and practices from fields such as finance, state and corporate cybersecurity, and humanitarian operations. At the same time, I have also shown how civil society actors reconfigure different forms of anticipatory risk logics to reflect human rights and social justice. The next section of my conclusion gives a more detailed summary about the findings, theoretical contributions, and empirical contributions of the five core chapters.

Overview of findings in Chapters 4–8

In Chapter 4, I introduced my approach to studying the anticipatory dimensions of resistance to contemporary surveillance. In this chapter, I explored the anticipatory dimensions of two practices: threat modelling and risk assessment. I looked at how these practices are explicitly structured to guide action amidst surveillance uncertainties. I investigated how they allow civil society actors to weigh the likelihood of imagined potential future data harms, articulate situational contingencies, and map these contingencies to appropriate counteractions. I looked at how they thus function as a heuristic aid for choosing practices and 'tools' to counter concerns about surveillance and datafication. My **contribution** with this chapter was to unite critical data studies literature on data practices with the study of risk and anticipation through a novel concept. This approach drew attention to the future-oriented dimensions of practices that counter and mitigate the threats and harms of

contemporary surveillance. I did so through my proposal of the term **'anticipatory data practices'**, which I use to describe practices such as threat modelling and risk assessment. I conceived of anticipatory data practices as a hybrid concept that brings literature on the politics of risk and threat construction into conversation with studies of everyday technology use. To accomplish this synthesis, I connected Anderson (2007; 2010) and Alvial-Palacino's (2016) notions of 'anticipatory practices' with 'data practices' (as conceived in critical data studies) in order to describe practices which grapple with 'data mess' through anticipatory modes (c.f. Pink et al., 2018). Through this exploration of anticipatory data practices, I also sought to contribute to critical security studies literatures concerned with preemption and anticipatory regimes by showing how anticipatory logics are appropriated and reconfigured by civil society actors working beyond the State and the corporation.

I explored anticipatory data practices within the context of shifting civil society priorities, highlighting how a disillusionment with inadequate existing technical 'solutions' to surveillance drove a shift amongst digital security practitioners to address worries and concerns of targeted communities. As I showed, this shift involved moving from universalised conceptions of surveillance as a ubiquitous and inescapable reality, to a situationally contingent concern. The shift towards contingency, in turn, gave threat modelling and risk assessment methodologies greater importance as tools to help people determine how to find safety amidst probable surveillance. Hence, I argued that the increased importance of practices such as threat modelling can be connected with a growing understanding that there is no generic technical solution to surveillance. I then related the anticipation of surveillance-related harm with the politics of expertise and diversity within civil society.

I also highlighted the increased attention within civil society to issues of diversity and representation, the mainstreaming of feminist epistemologies (and the contradictions which come with this mainstreaming), and the increased professionalization of security and safety work.

In **Chapter 5,** co-authored with Stefania Milan, we introduced the notion of algorithmic **'counter-imaginaries'** to discuss how dominant commercial and state imaginaries of datafication are contested by civil society. Together, we addressed the emergence of counter-imaginaries within civil society's commitment to oppose dominant imaginaries of datafication as constructed by state and corporate interests. We also **constructed a heuristic** to help conceptualize how and why civil society actors have shifted their approaches to mitigating threats and contesting technological harms over the years. This heuristic broke down civil society responses to the threats of surveillance into three categories: stabilized, formative, and speculative. These categories describe the degree to which civil society actors have tamed and domesticated problems relating to digital security, privacy, and safety through particular technical 'solutions'. Constructing this heuristic was a way for us to tackle a question central to the larger, collaborative DATACTIVE ERC project, which was: **how do techniques and strategies of surveillance resistance shift in response to datafication?** In thinking through this heuristic, we sought to capture moments of disjuncture in civil society repertoires for addressing surveillance and data concerns. We understood these moments, during which particular problems and 'solutions' to the harms of surveillance and datafication collapse in relation to new threats and priorities, as leading to a change in resistant practices. To explore this change dynamic, we conducted three case studies of software projects. The

first case dealt with new computing systems meant to mitigate the sophisticated security intrusions of state actors; a second case sought to intervene into the data exploitation that comes with Internet of Things networks; and a third case tried to prevent human faces from being turned into templates for widespread 'smart' facial recognition. These cases drew from data I collected for my thesis, as well as a focus group that Milan led with the developers of Dowse, one of the three featured projects.

We then identified how these three projects embodied the algorithmic counter-imaginaries of compartmentalization, awareness, and obfuscation. First, we explored the possibilities and limits of compartmentalisation as a software strategy and user practice operationalised by QubesOS. We showed that, on one hand, isolating different parts of a computing system (and computing practices) could help create 'safer' spaces for computing, in line with digital security priorities common to hackers and technologists. However, we also demonstrated that, in the practice and perspective of the software's users, it did little to guard against the corporate exploitation of data. Next, we investigated Dowse, an intervention into consumer IoT technologies. Here, we explored how technologists and security specialists draw on the ambivalent promise of 'awareness' in order to increase knowledge of threats. Our third case examined the use of CV Dazzle face paint by a group of human rights defenders and advocates concerned with the threats of facial recognition. We explored how CV Dazzle embodies the counter-imaginary of obfuscation as a way to sabotage data-driven biometric surveillances. Here, we again showed that the concept and practice of obfuscation provides a path of possibility beyond the capture of a particular form of surveillance, at the same time that its tactical utility remains quite limited and fragile. In summary, we

drew on this data to challenge the way that dominant imaginaries of datafication configure users as 'either co-producers of surveillance or its helpless victims'(104)

In Chapter 6, I returned to my exploration of risk assessment methodologies to focus on how risk assessment is enacted as an embodied, situationally specific practice in the context of a digital security training for human rights defenders. Drawing on data from participant observation, I explored how risk is constructed through an intersubjective, collective process of grappling with the uncertainties of surveillance and digital threats. My theoretical contribution with this chapter was to unite valuation studies (a subset of the field of STS) with critical literature on risk management through the introduction of my concept of '**Qualculative Convergence'.** This concept provides a way to understand how uncertainties related to surveillance are transformed into manageable risk. The concept of qualculative convergence draws on valuation studies (Callon and Law, 2005; Cochoy, 2008) to provide a way to capture the processual elements – both the quantitative 'calculative' logics and qualitative forms of judgement – that go into taming uncertainty. I use the concept to describe the intersubjective process that a digital security trainer and a group of human rights defenders draw on to turn data 'mess' and conjecture about undesirable security futures into a scientized heuristic for decision making.

As I described, the process of qualculative convergence unfolds across three stages: first, a digital security trainer establishes shared definitions of security and technology. Second, the trainer elicits stories about threats and concerns to synthesize the experiences of the group of people they are working with into a legible notion of risk. In this particular training, this process of synthesis occurs with

the use of a risk matrix – a visual risk analysis tool that organizes and mitigates the vulnerabilities of daily life by different degrees of severity, impact, and degree of possibility. In the third stage, particular security mitigations are chosen and plans are made to implement them beyond the training space. The goal is to come out of such a training with a repertoire of strategies and tactics to mitigate the harms of digital threats, so that 'at the end of [the training] the individual can act' (Interview #12). In the chapter, I argued that my concept is a necessary intervention into rationalist discourses of security risk as a naturalized, pre-existing thing in the world – a discourse prevalent in commercial cybersecurity and enterprise risk management. In making this argument, I further a goal of this thesis: to de-centre state and corporate discourse about risk and security.

In Chapter 7 I investigated an imperative within civil society to develop collective infrastructures capable of facilitating rapid response to digital threats such as malware attacks, disinformation campaigns, and online harassment. Here, I delved into the role of anticipatory practices in the infrastructuring of digital security. I explored new forms of information infrastructures developed to facilitate the collection and sharing of data related to probable threats, looking at how threat information sharing standards and infrastructures emerge from collaboration and contestation amongst commercial and state cybersecurity actors and security specialists working with targeted communities. My contribution in this chapter is to introduce and develop the concept of **'anticipatory security infrastructures'**, which I defined as diffuse, relational information infrastructures developed by multiple communities of security practice to predict, block, or develop resilience to anticipated future surveillance and data-related harms. This concept sits at the

intersections of contemporary studies of data infrastructures, cybersecurity, studies automation, and critical studies of data practices. I examined the contestations that go into processes of anticipatory infrastructuring, looking at how civil society practices both challenge and appropriate conventions and practices from the commercial cybersecurity realm.

Further, I investigated a desire by security specialists to automate security and more precisely predict future security threats in the service of greater efficiency. I looked at how the desire to automate security manifests within civil society organizations concerned with responding to the digital quandaries, threats, and harms affecting non-profit organizations and social movements worldwide. In exploring the politics of security infrastructuring, the chapter identified and analysed two contrasting approaches to threat anticipation. The first 'global' approach is premised on the application of data-driven security techniques; automated security anomaly detection; centralised data governance, and a rigid understanding of what constitutes 'good' and 'useful' data in the context of security. I contrasted the global approach with a second, 'local' approach rooted in feminist and autonomous approaches to security and data. I examined how the local approach to threat anticipation respects the heterogeneity of security as a concept and practice; allows for communities engaged in security infrastructuring to flexibly encode and recode data standards; and to define for themselves what security and safety mean in the context of their work. I explored the political importance and ramifications of these two different approaches for civil society digital security as well as commercial and state cybersecurity.

In **Chapter 8,** I explored paths to countering the logics of preemptive surveillance, looking at how the preemptive techniques of police and security actors are interrupted by targeted communities through daily security practices and abolitionist social justice organizing work. My contribution with this chapter was to provide a rich account of how preemptive logics are resisted, something which scholars of technology and society have argued demand more attention (Andrejevic et al; 2020). My focus in Chapter 8 was on understanding two strategies of resistance to preemptive surveillance: resilience (as embodied through structured digital security protocols for preparedness) and refusal (as embodied through abolitionist social justice organizing). I looked at how these two strategies draw on 'proactive', anticipatory action to disrupt the paranoid racial temporality of preemption. I drew from my thematic analysis of interviews and fieldwork material to highlight the widely expressed sentiment that to counter preemptive surveillance, it is **necessary to act 'proactively**'. The chapter explored proactivity as an anticipatory orientation that captures an imperative among social movements to regain the time-space of the 'not-yet' from preemptive actors seeking to surprise and disrupt the actions of their subjects. In exploring how preemption is resisted, I showed how the anticipatory logics of opposing actors refract in contentious and violent circumstances, calling attention to the bizarre cycles of anticipation and counter-anticipation that result from the harms of preemptive policing and security.

I explored proactive strategies of resistance to preemption in two contexts in which human rights defenders and social justice organizers directly challenge the carceral, preemptive regimes of contemporary policing. The first case of the chapter went to the site of a digital security training for human rights defenders, where I

described a security preparedness exercise intended to help human rights defenders understand how to cope with preemptive office raids against human rights organizations. The second case explored proactivity as enacted by grassroots community organizers in the United States working to abolish predictive policing. In this second case, I provided an account of a contentious discussion taking place between an organization challenging predictive policing paradigms in Los Angeles and an audience of digital security specialists at an international digital rights and Internet freedom conference. I concluded by exploring tensions between the experiences of social justice organizers countering predictive policing and data-driven discrimination with experiences of security specialists and human rights defenders focused on digital security and 'digital threat response'. I critically reflected on how resilience and refusal lead to different prefigurations of the future, probing the differences in abolitionist approaches to community organizing against technological harms and the managerial approach to digital resilience being promoted by security specialists through an intensified focus on digital security protocols.

Summary of theoretical and empirical contributions

In this section, I provide a broad summary of my theoretical and empirical contributions in relation the fields of study I engage with.

Contributions to the critical study of anticipation, surveillance resistant practices, and agency in a datafying, automating society

In recent years, scholars exploring contemporary surveillance and automated systems have interrogated an increased focus on the predictive and preemptive logics imbricated into the automated systems being deployed by institutions across different social realms. The fields of critical data studies, surveillance studies, and critical security studies have by now extensively explored different forms of anticipatory surveillance, intelligence-led policing, predictive policing, predictive data analytics, and algorithmic risk scoring. What remains under-explored in these literatures are the experiences of people living within, responding to, and countering the anticipatory logics that these systems enact. For example, while the field of critical security studies has devoted extensive attention to the preemptive logics of state and corporate security actors, there is a gap in understanding how actors working beyond the state and corporations make sense of these preemptive actions and respond with their own anticipatory actions.

I have thus argued that more research is needed that explores how different social groups respond to the anticipatory logics that characterize contemporary life with technology. In doing so, I have taken inspiration from Adrien Mackenzie's work on the anticipatory work of machine learners (2013; 2017) and Sarah Pink and co-authors' exploration of the 'anticipatory modes' bound up in banal data practices (2018). Like MacKenzie and Pink, I bring my focus of anticipation to the daily politics of practices and infrastructures engaging with data. However, unlike these two scholars, my research

particularly concerns the activities of civil society. As I argue, if contemporary life is now characterized by the encroachment of anticipatory regimes (c.f. Adams et al., 2009), it follows that it is essential to ask how anticipatory logics suffuse and shape the lived experiences and actions of citizens, targeted groups, and groups that strive to advance human rights and social justice. In this thesis, I have advanced this area of questioning by investigating the refraction of anticipatory logics as they move from state and corporate realms into the realm of civil society, and back through practices that appropriate and reconfigure anticipatory logics. My contribution to this discussion is to advance anticipation into the study of civil society practices that seek to counter surveillance harms.

My research findings show that groups affected by surveillance and data harms are enrolled into anticipatory logics to try to avoid future harms. I show that this enrolment results in new commitments and pressures, such as an individual and collective focus on maintaining continuous awareness of potential threats, as well as an investment in data-driven security and resilience. In Chapter 4, I trace how security educators working with targeted communities import anticipatory conventions from other sectors concerned with risk and threat management. In the process, they enrol those they work with into their logics to advance changes in the security practices of affected communities. I argue that these commitments and their accompanying pressures 'prime' targeted communities to continuously scan for future threats. In turn, scanning has a cascading effect, resulting in a felt imperative to act 'proactively' against probable harm, as respondents describe in Chapter 8. Across this thesis, I also show several ways that individuals and groups reconfigure hegemonic anticipatory logics, even as they also import them into their work from actors antagonistic to their interests. In

Chapter 8, I show this reconfiguration in my study of the imperative to act proactively against anticipated harm, and how it informs efforts to reclaim the time-space taken from targeted communities by violently preemptive security actors and police. In chapter 8, I draw particular attention to abolitionist strategies of refusal to technological harms. I look at how community organizers engaging in abolitionist work actively prefigure more just futures by challenging the foundations of institutions engaged in preemptive violence.

In addition to contributing to critical studies of anticipation, risk, and data practices, this thesis also contributes to literature that focuses more broadly on surveillance resistance and civil society. I provide a thematic analysis of shifting priorities and problem definitions amongst transnationally coordinating non-profit organizations and grassroots groups engaged in countering the harms of surveillance, contributing to studies of activism. With my empirical data, I capture how attitudes towards surveillance and datafication have shifted in relation to changing threats. Because my thesis implicitly deals with the temporality of threats, it's notable that the period of my research saw radical changes in the attention economy and public discourse of issues and problems related to datafication. This change was reflected in the concerns of interview respondents and in my fieldwork sites. At the beginning of the PhD project in 2015, the issues discussed across different sites of fieldwork revolved around big data and emerging best practices of digital security. In the last years of the project, the discussion saw an increasing focus on AI-driven surveillance, data-driven discrimination, and automation.

This shift in the attention economy exposed a deep tension between the need to attend to persistent everyday issues – such as funding,

resource constraints, and information management – and the need to monitor emerging threats and concerns – such as new information control laws, new automated surveillance architectures, and the ever-evolving techniques of exploitation of computing systems by states and corporations. Additionally, this thesis documents increased professionalization and specialization of different forms of security work in civil society, along with a formalization of information infrastructures intended to help mitigate threats. It is important to note that despite a shifting landscape of threats, fundamental concerns about daily safety and security remained constant between 2016 and 2019. Basic digital security protocols relating to secure storage and communication remained necessary, yet difficult to integrate into the socio-material demands of daily work, even as some tools and platforms changed. Funding for civil society initiatives and alternative technological infrastructures remained scarce, and concentrated in the 'global north', though civil society has undertaken efforts to decolonize and redistribute resources more equitably. Together, these empirical findings about civil society demonstrate that in addition to capturing changes in technologies and threats, it is also important to understand what kinds of problems persist, and to 'stay with the trouble' they present (c.f. Haraway, 2016).

Contributions to critical study of digital/computer/cyber(securities) and risk

In exploring the anticipatory dimensions of resistance to surveillance, my thesis has devoted much of its attention to the practices and infrastructures of 'digital security' as conceived by

civil society actors such as NGOs, technologists, and security specialists working to develop mitigations to digital intrusions, online harassment, and other forms of targeting by states, corporations, and antagonistic actors. Integral to my investigation of digital security has been the continued contestation around its scope of concern. In other words, what counts as a security concern and what doesn't? To what degree do and should security concerns overlap with issues around corporate data exploitation and data-driven discrimination? Where does civil society digital security end and commercial and state cybersecurity begin? My exploration of the contested boundaries of security(s) in turn allowed me to trace how anticipatory logics and practices are continuously appropriated and reconfigured across different social realms. Considering my interest in how practices travel, this section of the conclusions chapter explores the relevance of my research findings for contemporary debates on security beyond the realm of civil society.

As I have come to the end of my time working on my thesis, I have enjoyed the opportunity to discuss my findings with several generations of academics and security experts focused on the study and practice of technology and security. Through these discussions, I have learned that my research findings are highly relevant to a new field of security studies emerging from two decades of technical usability work, seeking to understand the 'human' dimensions of security (Adams and Sasse, 1999; Whitten and Tygar, 2005). Situated at the crossroads of computer science, cognitive science, psychology, and international relations, this emerging field organizes its concerns around the notion of 'socio-technical security' (Ferreira et al., 2014; Kroeze, 2017; Mujinga, Eloff, National Cyber Security Centre, 2020). Since 2014, socio-technical security has been actively developed in the US and the UK at academic and policy-oriented

institutions concerned with cybersecurity, critical infrastructures, and national security. The field works from the relatively newfound acknowledgement within technical security disciplines that there is no simple separation between 'technical' and 'social' issues. Socio-technical security tries to flip the longstanding computer security trope that 'humans are the weakest link' in the so-called security chain (Schweitzer, 2003). It recognises that, in light of continued human failure to perfectly configure security technologies, it is the systems that must be changed, rather than the people. This is quite an important step within a field long dominated by a limited understanding of the inextricable sociality of technical practice and infrastructure.

While this acknowledgement is hopeful for advocates of human-centred and 'humane' approaches to technology development, I also observe that many projects developing socio-technical security approaches risk replicating the very tropes that have contributed to the fields' deterministic approach to understanding sociality. For example, I note that in US and UK discourse around socio-technical security, there is a tendency to simply transplant this new conceptualization of security onto national security and the intensifying 'cyber' domain of international relations and warfare. After this transplantation, socio-technical security still carries the militaristic undertones that shape corporate cybersecurity and state national security. As a critical security scholar and human rights and social justice advocate, I find this is concerning: in carrying forward such tropes, this emerging discipline occludes the possibility of more explicitly connecting security to social justice and human rights. Indeed, the respondents interviewed in my thesis highlight that, rather than supporting human rights, the cybersecurity practices of states and corporations often become a part of the surveillance

regimes that they are trying to contest. Therefore, I argue that, while the re-conceptualization of security as socio-technical is an important development, it should be understood as a starting point rather than an endpoint in understanding how we should relate questions of security to social justice and human rights.

Considering these concerns, I hope that the findings of my thesis may serve as a humble counter to corporate and state-centric cybersecurity discourses that currently inform the growing study and practice of socio-technical security. In a time in which cybersecurity has turned into a hegemonic formulation of security amongst states and corporations, and become subsumed into militarized discourse, becoming an intrinsic element of warfare, I seek to highlight the plurality of security and to critically interrogate what constitutes security and safety, and for whom. As made plain across the chapters of this thesis, security can mean many different things, as its meaning and practices are continuously contested by different communities of security practice. My research findings can be understood as a direct counter to rationalist, deterministic conceptions of 'behaviour' in relation to security. Unlike literatures that seek to understand security behaviour through cognitive constructs such as mental models (Wash and Rader, 2011; Blythe and Camp, 2012), I show that security practice is constructed through embodied experiences and situated knowledges. Rather than understanding security behaviour as an isolated, cognitive, or psychological phenomena, I demonstrate the intersubjective processes of sense-making and threat construction that go into defining what constitutes a threat or a risk.

One of the goals of my thesis is to highlight the importance of alternatives to state and commercial-centric conceptualizations of

cybersecurity. Towards this goal, I explore how, in a world of violent state centric security, digital security trainers in civil society consciously depart from reproducing securitized and militarized discourse. For example, in Chapter 4, I show how feminist epistemologies influence security practice. Chapter 4 discusses a symbolic intervention into the word 'security' made by a group of educators who call themselves 'holistic security trainers'. In their work, they suggest that this word can be replaced with a care-oriented notion of security, which they call 'wellbeing in action', drawing inspiration from feminist poet and scholar Audre Lorde. This chapter also looks at how the holistic security methodology decentres the expectation that civil society actors concerned with surveillance and digital threats must achieve an all-encompassing 'situational awareness' (Suchman et al., 2017) in order to find safety. Instead, holistic security trainers put the locus of security analysis on the somatic experience of security and insecurity, in accordance with a feminist emphasis on embodiment. In Chapter 7, I highlight the importance of security actors often left out of high-level policy debates and computer science literatures on security. In particular, I point to the work of grassroots feminist groups and women's rights organizations, which develop feminist threat counter taxonomies to better reflect the realities of gendered violence. I look at how such feminist security framings oint to another way of infrastructuring cybersecurity and anticipating security threats.

In highlighting feminist practices and epistemologies and unexpected forms of security infrastructures, I aim to complicate and decentre state and corporate centric narratives about security and technological progress more generally. However, the narratives of security that I present are complicated. In foregrounding the ways that civil society digital security overlaps with and diverges from

hegemonic conceptions of cybersecurity by states and corporations, my research highlights many instances in which commercial cybersecurity and civil society responses overlap and cross-pollinate, despite differences in politics and priorities. This overlap is a focus of Chapter 7, in which I explore how civil society actors take inspiration from and collaborate with the commercial cybersecurity industry on threat intelligence information sharing to better anticipate threats. I have sought to highlight the important discussions and problem definitions left unadressed by both civil society digital security and state and corporate cybersecurity. For example, in Chapter 5 I describe the artificial disjunctures created between security and related areas of concern about technology-related threats. I show that for people grappling with the uncertainties of surveillance in an era of datafication, it can be arbitrary and counter-intuitive to separate issues of security from issues of privacy, data exploitation, and data-driven discrimination. I thus argue for the acknowledgment that security is inextricable from the intersecting technological problems and social justice issues.

Having summed up my contributions to several fields and sets of literatures, the final section of my conclusions chapter ties my research findings back to my own long-standing questions and concerns as a practitioner. Through this synthesis I also offer clues for thinking about potential paths of action that might take us beyond the anticipatory regimes and the hegemony of risk-centric logics that characterize our datafying society.

Towards a critical politics of anticipation in the datafied society: connecting past, present and future threads on surveillance resistance and security threats

In March 2021, I was honoured to be invited into a rich reading group to discuss Chapter 4 of this thesis, published as 'It depends on your threat model: the anticipatory dimensions of resistance to contemporary surveillance' in *Big Data & Society* that January. To remind the reader, in this chapter, I examined the importance of threat modelling and risk assessment as anticipatory data practices. As I showed in the chapter, many digital security specialists working to support human rights and social justice rely on risk assessment and threat modelling methodologies to tame the uncertainties of surveillance and mitigate digital vulnerabilities that arise in daily human rights- and social justice-focused work.

The reading group meeting was organised by a group of academics studying security from a critical, interdisciplinary perspective. One of my respondents was a policy-focused scholar who expressed concern that my article was too enthusiastic about security risk management tactics and strategies in the context of pushback to surveillance harms. The scholar argued that individualized practices of risk management have inherently limited potential to solve the structural and institutional issues that produce the harms of concern. I responded to the scholar that I am in deep agreement with their view on the limits of risk management and related self-defensive actions as avenues for contending with 'structural' harms. Indeed, my thesis takes a critical perspective on individualized responsibility,

as embodied in many practices concerned with security and risk management. Across the core chapters of this thesis, I show that while risk management strategies can serve to 'tame' certain problems and make them feel more manageable, there is a world of difference between managing or mitigating risk, and doing away with its source. One of the concerning aspects I observe with regards to anticipatory practices such as risk assessment and threat modelling in the context of civil society work is how they arise from a responsibility born by targeted communities to maintain continuous awareness of potential surveillance threats. I thus investigate how future-oriented thinking focused on risks and threats can intersect with (and even augment) violent master narratives about technology and innovation.

I believe the confusion about my positionality towards risk management might stem from the thin line I have toed with my thesis. I have worked to simultaneously show why certain practices become necessary, while also pointing to their frictions, disjunctions, and capture into hegemonic regimes of security, risk, and anticipation. Just as my thesis raises the above critical concerns with anticipation and risk, I also show that thinking and doing through the lens of risk remains deeply useful and even necessary, and that it can be quite difficult to move beyond it. In this regard, I argue that it is important to remember why the people interviewed for this thesis turned to risk assessment and threat modelling practices in the first place. This point was best articulated by a respondent featured in Chapter 4, who works both as a policy advocate fighting to regulate biometric technologies, and as a digital security trainer teaching individualized tactics of self-defense, including threat modelling and risk assessment. When I asked her whether she sees one mode of

work more necessary than the other, she responded simply, ‘we need all the tools’ (Interview #41).

This advocate and trainer further argued that it would be an arbitrary exercise to try to make a hierarchy of usefulness around different tactics and strategies (such as between individualized tactics of risk assessment she teaches in digital security trainings, and the advocacy she engages with around high-level policy arenas). She noted that in her work across Central America, there were times and places where a particular form of intervention in technological threats and harms suddenly became impossible to actualize due to the surrounding sociopolitical and technical context. When this happened, she found it necessary to ‘reach into the toolbox’ (Interview #41) and draw on a tactic or strategy that would fit local constraints. In some cases, this adaptation meant doubling down on daily safety and security practices. In other cases, her focus became to advocate for a particular law or policy. Her explanation, in turn, reminds me of a long-time human rights advocate who I had the honor to informally correspond with over the years I worked on my thesis. This human rights advocate has devoted most of her career to providing practical lifesaving support to a small group of human rights defenders living within an increasingly isolated and totalitarian regime. Her support includes provisioning custom technical mitigations for continuously shifting information controls, and providing emergency legal when people are arrested. She told me that over the years, she has regularly been asked by funders why it is worthwhile to continue devoting funds to a form of work that doesn’t seem to ‘scale’ beyond the small groups she works with. She likes to remind those who will listen that ‘whoever saves one life saves an entire world’, quoting Talmud Sanhedrin 4:5. From her vantage point, it seems that while broader fights are fought, it remains necessary to attend to individual lives

and the banal nuts and bolts that make the continuation of their fights possible. I believe the experiences of these two people demonstrate that there is no either/or when it comes to exploring paths beyond our current predicaments with technological harms. There is simply no clear line of separation between day-to-day practice and fights for structural change. The more we strive to understand their interrelations, the better we can imagine emancipatory avenues for engagement with technology.

I acknowledge that the ambivalent picture I present of resistance and risk may not be satisfying for those seeking to measure and compare different strategies of resistance to surveillance and technological harms. Yet, important truths are found in exploring this ambivalence (c.f. Eubanks, 2011). Over the course of my work on this thesis, I have reflected on my own ambivalent relationship with risk management, and my absorption into various forms of anticipatory regimes. Despite my intellectual interests in critiquing risk, explicitly risk-centric language and risk assessment has become an increasingly important tool in my life, especially since the start of the COVID-19 pandemic, which coincided with the final stages of writing. I belong to a cohort of people billions strong that is deemed by certain risk rubrics to potentially be ‘at risk’ of serious COVID disease. Every day since mid-February 2020, I have reflected with ambivalence on my position as someone so labeled and absorbed into a particular regime of risk-based governance and anticipation. The anticipatory regime at play for me in the context of this pandemic is a self-constructed one. It involves little automation, and there is no single disciplinary overseer managing my every move. However, it is an anticipatory regime I have been responsibilised into, in order to cope with my everyday safety concerns in the absence of much protection from above. This anticipatory regime rests on my ability to rapidly

adjust my safety strategies amidst scientific uncertainty and confusing public health messaging, and also hinges on my reluctant consent to be labeled an ‘at risk’ person, one I have consented to because it has promised to afford me certain kinds of care from the public health system of the country where I reside. Unfortunately, the experience of many shows that the designation of broad swaths of the population as being ‘at risk’ serves to justify the austerity logics and necropolitical agendas, while care remains elusive. As a result, I am not satisfied with carrying this risk label. Still, if you ask me how this pandemic has treated me, I will probably preface my response by noting that I am at risk, which speaks to my ambivalent absorption into ways of doing and being that I find problematic.

Drawing on this personal reflection, I think it is important to remember that many of the people I have interviewed for my thesis have come to use risk assessment strategies in situations where they have been made responsible for their own protection. As I have argued throughout this thesis, methodologies of risk assessment and threat modelling provide a way to tame the uncertainties of contemporary surveillance and to establish concrete heuristics for action taken in the name of safety, when safety is not forthcoming from states or corporations. That people now embrace such tools as risk assessment and threat modelling can be understood partly as the result of a failure in duty of care at a state level. Going further, the embrace of these practices can also be understood as a direct result of active state spying and intrusion into civil society work. For this reason, I cannot negate the importance of risk management in the daily practices of people trying to strive for social change for the same reason I cannot negate the usefulness of being able to call myself ‘at risk’ in the middle of a pandemic. I believe that the importance of risk management and tactics that tame uncertainty

must be acknowledged as having a place in a larger politics of data. At the same time, I believe it is the responsibility of people charged with spreading awareness about technological concerns and working with communities to mitigate threats and be mindful of the problematics of risk and anticipation. This is especially the case because risk assessment and threat modelling often continue to be expert-led activities. As I show in Chapter 4, the experts teaching these methods play an important part in enrolling people into anticipatory logics, a process that creates new commitments and responsibilities. Considering the crucial concerns I have highlighted regarding risk and anticipation, I think it behooves such people (myself included) to also explore how we might be able to move beyond risk.

Over the years that I have documented shifts in civil society and its threats of concern, I have observed that the problematics of risk and the hegemony of risk regimes have become a central area of contestation in local and international discussions about the governance of artificial intelligence systems and their harms. Community organizers and activists fighting against the harms of carceral systems explicitly draw links between institutional approaches to risk management and individual lives framed as 'risky' and 'at risk', critiquing the use of automated risk assessment strategies within data-driven policing and in the judicial realm. Arguing that it is not acceptable for our institutions to make risk subjects out of Black communities in the United States, Data for Black Lives Founder and Executive Director Yeshimabeit Milner asks: 'how did the word risk – which finds its origins in finance and insurance, become a label for people like me and my friends?' (Milner, 2019). The growing recognition of the hegemony and harms of risk-centric thinking and systems, I believe, is why the vital and

long-standing work of abolitionist, anti-racist organizations such as Data for Black Lives have received increased amounts of attention in public debate and in academia. Now, community organizers argue that it is essential for this wider attention to be channelled towards co-liberation. This leads me to ask: what is my small part in this broader conversation? For my part, I argue that even as we continue to frame our lives through future-oriented logics such as risk, we should find ways to intervene in the hegemonic risk logics and risk rubrics that our lives are fitted into. But how? Per Amsler and Facer (2017):

> liberating the future from... the epistemological grip of the anticipatory regime is not a matter of identifying existing possibilities that can be successfully predicted given what is already known, but an experimental process of generating and enlarging the space of possibility itself through practices of critical, disobedient anticipation (13).

This leads me to ask: what does critical, disobedient anticipation look like? How might it be possible to live in anticipation and shape one's life around the avoidance of undesirable futures – while also carving space out to prefigure another world? My thesis shows that human rights defenders, security specialists, and social justice organizers are already carving out spaces of possibility through their practices, but there is more work to be done. For my part, asking this question brings me back to my original motivations for undertaking this thesis. As I mentioned in the introduction and literature review chapters, this research originated in my work as a critical practitioner of digital security, during which I began to question my reliance on risk as a lens for understanding and acting in the world.

As mentioned in the introductory chapter of the thesis, my work in civil society digital security involved engagement in an action-oriented research project aiming to increase the field's understanding of the sociotechnical issues that make digital security a challenge for human rights defenders. Here I come back to it to highlight a small effort I made with a colleague to critically disrupt risk-centric language.

Working together, my colleague and I conducted several digital security trainings to surface the most pressing digital security-related concerns for three groups of human rights defenders in South Asia, Central Asia, and Southeast Asia. During our planning discussions, we decided to conduct a small experiment on how we – as digital security practitioners – talk and think about risk. Our experiment was to try to avoid using the word 'risk' as much as possible when engaging in discussions with human rights defenders. We reflected on the fact that 'risk' can make the embodied experience of danger more abstract, and thus can obscure the sources of the danger that had made our work on safety and security important in the first place. As anthropologist Mary Douglas argues, risk-centric language can entrench and encourage market-delimited problem definitions, framing the worthiness of lives as a matter of cost-benefit analysis. Further, risk -centric language can contribute to transforming institutional accountability crises into issues of individual responsibility, thereby contributing to the reproduction and re-entrenchment of austerity logics. My colleague and I thus asked ourselves: what work was the word doing when we said risk but meant danger, violence, oppression, precarity, scarcity, austerity, or corruption? Our avoidance of risk language was part of a broader effort to avoid language that responsibilises people for their safety and security (c.f. Gürses, 2014; Kazansky, 2015).

Instead of using 'risk,' we agreed to try contextualizing concerns about digital surveillance and insecurity in relation to structural inequalities, political instability, social inequity, and the everyday resource constraints that make technology challenging. Rather than focus on a false notion of absolute security and safety, we tried to work backwards from the larger goals of the people we worked with to create situationally appropriate strategies to increase safety. Our goal was to see if we could use avoid the word risk entirely during our trainings and discussions with human rights defenders. In our workshops, we talked about context where we would have discussed risk, and we conducted a participatory 'context analysis' instead of a risk analysis (Kazansky, 2016). The report that emerged as an outcome of this work similarly tried to avoid the word risk. Our intervention to break our reliance on risk was a small step to re-imagine how we talk, think about, and respond to injustice and harm, an example of a 'small p politics' way of intervening in hegemonic notions of risk and security. But what about intervening in 'big P politics'?

I argue that the intervention my colleague and I made can be understood as a small-scale corollary to a current fight playing out in the European technology policy space. On the heels of seemingly unending crises of accountability surrounding big tech companies and artificial intelligence, as of July, 2021 the European Union (EU) is going through the process of adopting a new framework to help it better deal with the threats and harms of artificial intelligence. This new framework is premised on a risk heuristic that breaks down artificial intelligence systems into levels of concern from 'unacceptable' to 'minimal risk'. Drawn as a pyramid, the 'unacceptable' domain for AI use is the smallest – representing the tip of the pyramid – and is designated as the part of the pyramid

where new regulation is most necessary. Meanwhile, the 'minimal risk' domain is the largest on the pyramid. The implication is that most AI risks can be countered through self-regulation. In response to this proposal, civil society organizations have spent the better part of 2020 and into 2021 arguing against risk-centric conceptualisations of AI harms. Digital rights civil society organizations such as Access Now call this risk framework an arbitrary exercise that gives too much room for self-regulation to potentially harmful systems. They also believe it ignores how data exploitation and automated systems can have existentially serious impacts even across 'minimal risk' domains of AI use. To counter the EU risk framework, civil society organizations instead call for the establishment of human rights-based 'red lines' approach to guide acceptable and unacceptable AI use. The idea is to draw clear lines beyond which any AI system with clear human rights impacts should be banned, rather than simply tamed through regulation. I believe the push by civil society organisations for a rights-based approach to AI regulation is a crucial intervention, and I see it as a high-level corollary to what my colleague and I tried to do on a very small scale with individuals and organisations concerned with their digital security.

By sharing these examples, I highlight that there are many ways to disrupt risk, whether by experimenting with risk language substitutes in digital security trainings, calling for red lines instead of risk rubrics in high-level policy fora, or pushing for the dismantlement of risk-centric carceral systems. Engaging critically with issues of risk at these different scales is a way to work towards 'enlarge(ing) the space of possibility' (Amsler and Facer, 2017) for more just futures. By challenging how institutions and communities construct risk, we can find ways to refuse and interrupt the anticipatory surveillance regimes that we live within. Further, by finding strategies to

challenge risk- and future-oriented logics, we can also challenge deterministic narratives about people and technological systems. This, in turn, has the potential to make our technological systems and societal institutions better able to hold space for indeterminacy, substantively grapple with the root causes of uncertainty; and engage with the world in more just ways. In the words of anthropologist Anna Tsing, ‘indeterminacy, the unplanned nature of time, is frightening...but thinking through precarity makes it evident that indeterminacy also makes life possible’ (2015:34).