What harms may come?

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

Kazansky, B.

Publication date
2021

Chapter 1. Introduction

Introducing the research puzzle

On a sunny winter morning in 2016, a dozen digital security specialists based in Europe, the United States, and the Middle East and North Africa (MENA) region gathered around a long table in a rented event space on the edge of a central European city. The meeting was organized to discuss how to address threats of digital surveillance, online harassment, and technologically mediated violence faced by a loose coalition of 'transnational civil society' (Price, 2003) groups around the world fighting for human rights and social justice. The security specialists would spend the next three days around the table planning a new online digital security resource intended to help civil society actors, such as human rights defenders and journalists, learn how to mitigate the harms of profiling, harassment, and state and corporate intrusions. This was to be the first of many sessions soliciting input on how the resource should be structured and what should be included in its curricula. In the broadest terms, the focus of the resource would be digital security. However, the team building the resource was concerned about how to scope its curricula and guide its imagined users towards appropriate material for their situational concerns. At the core of the discussion was the question of what 'digital security' would constitute, and for whom.

'Digital security' is a term held close by civil society's digital security specialists concerned with mitigating the effects of a milieu of threats related to digital monitoring, intrusion, and technologically mediated harassment and violence (Access Now, 2018; Kazansky, 2016; Notley and Hankey, 2013; the Citizen Lab, 2014; the Engine Room, 2013; 2018). In the context of civil society practices, 'digital security' refers to a wide breadth of tools, techniques, and strategies for threat mitigation that are grounded in the daily technology troubles particular to NGOs and grassroots groups. While 'cybersecurity' has become the de-facto term used by states and corporations to frame discussions about technologically

related vulnerabilities and recourses against them (Veale and Brown, 2020), civil society actors have long taken pains to extricate security from its state and corporate-centric overtones (Hankey and O'Clunaigh, 2013; Radloff, 2013; 2018). In the context of civil society, many specialists deliberately distance digital security from militaristic notions of security and transplantations of geopolitical sovereignty into digital space. Civil society digital security is also contrasted with narrow, technically focused notions of 'information security' and 'computer security' (Nissenbaum, 2005), fields which, according to the respondents interviewed in this thesis, fail to concern themselves adequately with the human or social dimensions of security. Despite the clear disciplinary notions of civil society digital security, what it constitutes and where its boundaries lie is subject to ongoing negotiation.

The difficulty of bounding digital security came to the fore in the specialists' meeting I introduced above, in which a conflict arose over what topics should fit the curricula of the proposed learning resource. The team tasked with leading its development presumed that it would cover 'traditional' digital security topics related to the prevention of intrusions into digital infrastructures and the loss of data to theft and technical failure. To advance the project towards the goal of preventing intrusions and data loss, the team planned to cover how human rights defenders and journalists could improve their password management practices, learn how to identify probable malware and phishing attempts, and make use of encrypted communication and data storage tools. But no one in the room could come to an agreement on what specific tools or practices to feature, noting that each tool had its own flaws and vulnerabilities. Beyond disagreements over particular tools covered in so-called traditional areas of digital security, the specialists argued that the scope of digital security should be widened. They debated whether to cover issues such as digital literacy about 'how the Internet works' – including basic Internet protocol design and how digital data is routed from one computer to another – as well as social media safety (for example, techniques for how to set up and

manage multiple online personas in order to prevent the targeting of individuals trying to keep their identities hidden from antagonistic actors).

One specialist pushed to further expand the scope of digital security, arguing that the learning resource should also cover issues related to the platform governance of technology companies, and how individuals could avoid biometric surveillance, such as the mass facial recognition increasingly carried out in cities around the world. At this point, a conflict arose over the merits of trying to address threats that human rights defenders and journalists might not realistically be able to mitigate at an individual level. Should (and could) these concerns be addressed as part of a 'practical' curriculum? Beyond the 'what' of digital security, the 'who' was also subject to negotiation. Among the specialists brought in to provide input on the resource, most were there as proxies representing the interests of affected communities around the world. However, almost no one in attendance faced direct danger themselves. Instead, the attendees had become accustomed to be representatives of others – 'translators' (c.f. Star and Griesemer, 1989) for grassroots groups and social movements at the front line of justice and rights-based struggles. The discussion turned to those absent from the room; who would be the target audience of the learning resource? Anti-corruption activists in Southeast Asia? Human rights defenders in the MENA region? Women's rights activists in Central America? How might the 'needs' and interests of people from different regions differ? Should the resource aim for a 'universal' curricula or be tailored to particular affected communities?

It became clear to everyone seated at the table that it would be impossible to develop a resource able to adequately cover every potential threat for each possible audience. Thus, to scope and structure the curricula, one of the specialists presented the idea that the resource be organized around a heuristic of high, medium, and low risk. The idea was that each user of the learning resource could chose a risk designation that fit their level of danger and targeting, and be led to a cluster of appropriate mitigations,

somewhat like a ‘Choose Your Own Adventure’ book. The ‘high risk’ label, the specialist suggested, would refer to people under direct threat. He understood a direct threat as targeted intrusion into a computer, the exfiltration of sensitive information, a campaign of online harassment, or a death threat delivered through the email. The ‘medium risk’ label would refer to users that might feel they are potential targets but lack evidence that they under direct threat. ‘Medium risk’ was seen to map to suspicious events such as a suddenly slow computer, a clicking noise over the telephone wire, a strange car parked in the street outside the office, or a concerning new policy implementation. Finally, ‘low risk’ would refer to users of the learning platform who are engaged in political work but are based in places where rule of law is strong and civil society does its work unencumbered – even if, with every passing year, it has become less and less apparent that such a place truly exists.

At this point, one of the only people in the room coming from a so-called ‘high-risk’ context herself – a specialist from the MENA region who conducts digital security trainings – raised her hand to challenge this proposed risk heuristic. She argued that such an abstract distillation of danger and concern could not possibly align to the experiences of activists living in her country’s volatile political situation. With governmental actors introducing new surveillance technologies and reframing rights-based work as a threat to national security, she argued that an activist in her country might be a low-risk user one day and a high-risk user the next, and not find out until they are arrested, or worse. Further, she argued that the ethico-political dimensions of risk could only be understood within affected communities, not through a generic risk heuristic created by people far removed from them. Her comments surfaced an issue of epistemic injustice haunting this discussion of risk; to designate others as risky or ‘at risk’ is an act laden with power. This specialist alluded to something not feeling right to her about people sitting comfortably in an event space sorting and classifying the trauma and danger faced by people far away into neat rubrics.

The contentious discussion around risk and digital security that I have described here is one of many that I encountered in my thesis fieldwork. As I will show in this thesis, the question of how to effectively strategize against technologically mediated threats is one of ongoing importance and contestation. Blocking surveillance, intrusion, harassment, and other forms of violence through self-defence tactics is often paired with the mitigation of harms through 'risk management' strategies. Another strategy is to push for reforms of technology regulations, and yet another is to strive to abolish harmful systems at their institutional and societal roots. Such activities are all pursued, sometimes in close concert and at other times quite distant from one another, to counter probable threats and harms. As I make apparent throughout the thesis, this plurality of strategies is a result of the fact that there is no single 'solution' possible for complex societal issues of surveillance and technologically mediated harms.

One reason why there is no single solution is that the complexity of and deliberate opacity of surveillance techniques, algorithmic orderings, and data-driven processes makes it difficult to know how data is collected and exploited. Next, the brittle quality of technological 'solutions' available to address particular concerns shows there is no single 'effective' form of protection to potential harms, nor has a technology-driven approach succeeded in addressing the institutional and societal factors that create the problems civil society actors then try to grapple with. Finally, while some civil society actors call for more regulation of harmful technologies, there is no escape from the need for safety and security at an everyday level. Every instance of technology use by civil society groups may potentially threaten the capacity of civil society groups to continue their work – and thus also threatens the broader struggle for human rights and social justice. For this reason, digital security practitioners, human rights defenders, and community organizers around the world have become increasingly concerned with developing ever-more formalized, collective,

and anticipatory mechanisms to respond to probable technological harms – which I explore in this thesis.

In this thesis, I study the interrelations among different groups and individuals involved in grappling with the uncertainties, threats, and harms of digital surveillance. I study these interrelations as an institutional ecology (c.f. Star and Griesemer, 1989) of non-governmental organizations (NGOs), grassroots groups, security specialists, and technical service providers concerned with issues of human rights, social justice, and technologically-mediated harms. This institutional ecology arises from collaborations between groups with varying levels of institutionalization, geographic, scope, and political commitments. They come into relation with one another in order to counter the threats and harms of surveillance and related threats. Within this institutional ecology, I consider both people specializing in technology-related issues as well as those working on other issues who have become concerned with technology through their experience with harms. This latter group then comes into relation with tech-focused actors to mitigate these harms and prevent future threats.

I want to underscore here that contestations about how to respond to digital surveillance and digital threats are inextricable from the contested dynamics of 'civil society' itself. While many of the specialists described in the opening vignette often imagine themselves belonging to a larger field concerned with fighting for human rights and social justice in the context of technological change and surveillance, this field is highly heterogenous in its aims, politics, contexts, and institutional particularities. In this thesis, 'civil society' broadly refers to the realm of human action beyond the realm of the state and the market (c.f. Gramsci, as explicated in Sassoon, 2000). Narrowing this definition, I use the term civil society to refer to a loose grouping of transnationally coordinating non-profit organizations, grassroots groups, informal coalitions, and individuals working beyond the state and corporations to advance issues

at the intersection of human rights, social justice, and technologically related harms. Who considers themselves (or is considered by others) to be part of civil society is subject to continued negotiation. Some groups challenge the very notion of a 'civil society' altogether, instead preferring to talk about their work in terms of community organizing, movement-based work, and radical collectivities.

By way of example, one of the respondents interviewed in this thesis is a United States-based community organizer fighting for immigrant rights and supporting the Movement for Black Lives. This community organizer rejects the notion that they are part of a 'civil society', explaining that institutionalized civil society actors (in the form of well-funded NGOs in particular) are often implicated in the hegemonic patterns they want to change. The respondent called out the long-inequitable distribution of resources between larger, globalized non-governmental organizations in North America and Europe, and grassroots organizations worldwide; a homogenous and exclusionary culture of technologists and 'experts'; one-off style interventions organized by people from 'somewhere else'; and a failure to grapple with issues of racism and inequity endemic to civil society itself. The community organizer also objected to what they see as assumptions about participation within a liberal democracy, which they believe stands in the way of truly emancipatory politics. Explaining further, they said, 'civil society looks at democracies as civil and anyone outside as uncivil. So we're like, fuck that phrase, that means anyone outside is a savage, so fuck it' (field notes, 2018). Having spent years working within radical feminist communities in Europe, another respondent argued that in place of 'civil society' – even in the most 'radical', Gramscian sense – 'we need a better word' (Interview #40). Yet in an absence of consensus around a better word, many continue to use the term civil society to describe their larger field of work and to contextualize the communities they belong to. Hence, in this thesis I use the term civil society to very broadly situate its focus of study, adhering to the way that many individuals and groups interviewed talk about their

work. Beyond that, I stick closely to the self-descriptions and identifiers used by the different groups and individuals I have interviewed, who describe themselves as Internet freedom advocates, digital rights advocates, social justice advocates, human rights defenders, activists, practitioners, community organizers, technologists, intermediaries, translators, security specialists, hackers, educators, trainers, and facilitators. In the instances in which people have expressed an issue with the term civil society or explicitly defined their work through another one, I have foregrounded their preference and made it a substantive part of my analysis.

Inspiration for the thesis

Having introduced my research puzzle and discussed the relations and boundaries around some of the important definitions found in this thesis, I now explain how my inspiration for this thesis emerged from my own personal history engaging in civil society work. Since 2009 I have worked as an action-oriented researcher and educator in matters of digital literacy, privacy-enhancing technologies, and digital security (Kazansky 2015; 2016). Over my years in these roles, a recurring question in discussions with other practitioners was how best to break through the uncertainty that comes with determining how to respond as a community to surveillance and data-related harms. In these discussions, I often encountered the common answer that what to do in response to concerns over data and surveillance ‘depends on your threat model’ — an answer that highlights the contingency and uncertainty at play for individuals seeking safety in a datafied society. I took part in many impassioned discussions amongst security experts and human rights defenders about how to best talk about security risks: should risk be quantified? Is it ethical to frame life around threats and their probability of occurring? Should human rights defenders be made to feel scared to motivate them to protect themselves? Why don’t

people make use of the security and surveillance countermeasures that exist, and how can they be convinced to change their behaviours in response? These discussions revealed rationalist discourses, patriarchal models of risk communication, master narratives of technological use, and a contentious politics at play in the ways that risks, threats, and the uncertainty of surveillance are conceptualized by 'experts' involved in promoting and developing surveillance and digital security mitigations. As Scoones and Stirling point out, 'addressing uncertainty means confronting inequality, vulnerability, precarity and the deeply embedded inheritances of history head-on. Uncertainty is never just a technical issue' (2020:15). Yet, I found that due to the magnitude of uncertainties and harms many of us tried to address as a field, there was often a compulsion towards trying to 'tame' uncertainty through temporary fixes and heuristics that could provide some small sense of control in the immediate, as also observed by Aouragh et al., (2015). This is not to say that digital security is unnecessary or unimportant. On the contrary.

From 2013–2015 I lead an action-oriented research project that sought to answer how a burgeoning international community of digital security practitioners within civil society could better meet the digital security needs of human rights defenders targeted with surveillance. When this project was first handed to me, its goal was to better promote security 'behaviour change' within communities of human rights defenders. By the end, I had pivoted the project to investigate how structural inequities and political instabilities contributed to human rights defenders' lack of safety, and to what extent the countermeasures promoted by digital security practitioners and technologists helped mitigate them. The project provided an honest reflection on an uncomfortable question. Its main findings were that human rights defenders already put an enormous amount of energy into constructing safety strategies for themselves and their communities. Hence, the problem was not one of motivation or individual behaviour change. Rather, the technologies and pedagogies promoted by civil society organizations to help address issues of digital insecurity often

didn't stand up to their stated purposes (Kazansky, 2015; 2016). The main reasons for this failure included the brittle nature of promoted technologies and a lack of integration of technology concerns with the lived experience of human rights defender communities. This project caused me to reflect on how my practitioner community might contend with risk and uncertainty in more just, ethically, and politically congruous ways.

Formulating the central thesis question

Over time, my interests in uncertainty and risk crystallized into ideas for a critical project on the challenges of grappling with the uncertainties of contemporary surveillance. I was interested in investigating how – with all the different possible forms of monitoring and profiling enacted by corporations and governments – do affected communities determine which surveillance they must worry about? How do they form strategies of resistance in relation to the uncertainties of surveillance? To ask the question slightly differently, what are the practices that allow people to act in spite of the uncertainties of surveillance and datafication? These questions in turn crystallized the central question that guides this thesis: **how does transnational civil society grapple with the uncertainties of contemporary surveillance-related threats and harms?** My goal in exploring this question is to gain an understanding of how transnationally coordinating civil society actors –technologists, security specialists, human rights defenders and social justice community organizers – together negotiate the fight for human rights and social justice amidst the 'intrusive-unseen' uncertainties of contemporary surveillance, security, and data-related threats (Wang, 2018: 257). I investigate how resistance takes shape amidst the broader intensification of a participatory, data-driven surveillance society (c.f. Lyon, 2017).

For the purposes of this thesis, I decided to look at these questions as they applied to a transnationally coordinated ecology (c.f. Star and Griesemer, 1989) of civil society groups focused on providing support to surveillance-affected communities. Through a multi-sited ethnographic study of this ecology and its practices, I study how surveillance-related uncertainties are constructed, tamed, overcome, or made manageable by security specialists, NGOs, and grassroots groups through future-oriented practices embedded within daily work to support human rights and social justice. I particularly hone in on the 'anticipatory logics' that propel the enactment of practices and infrastructures used to prevent, subvert, or mitigate potential harms. I look at how the drive to anticipate and to take 'proactive' measures in the face of potential danger becomes a banal reality for populations concerned with the harms of surveillance and datafication. As I will show in the five core chapters of this thesis (Chapters 4-8), the desire to simplify data 'mess' and move beyond the uncertainties of surveillance is at the centre of efforts to counter the threats of digital surveillance. These practices of simplification are referred to by such terms as threat modelling and risk assessment. Threat modelling and risk assessment, as I will show, are part of a large and heterogenous cluster of 'anticipatory practices' (Anderson 2007; Alvial-Palacino, 2015). These practices try to convert an unwieldy and unpredictable mess of concerns into a manageable problem mappable to 'solutions' available to civil society actors concerned with their digital vulnerabilities. They come with various forms of epistemological baggage, as they are imported from other sectors concerned with risk management.

My exploration of anticipatory practices is guided by critical, ethico-political concerns related to the hegemonic anticipatory logics and anticipatory regimes (c.f. Adams et al., 2009) that characterize contemporary society(s). My concern lies with understanding the relationship between civil society's anticipatory practices and a broader

societal drive to predict and govern human behaviour through codified, data-driven, automated mechanisms for surveillance and social sorting (c.f. Gandy 1993; 2009; Lyon, 2002; 2014). In exploring how and why anticipatory practices are important to surveillance resistance, I investigate how they serve operational goals for safety while also potentially foreclosing particular political goals, due to the hegemonic epistemologies attached to anticipation across fields concerned with risk management, security, and governance. I also investigate how it might be possible to break from the hegemonic anticipatory regimes that characterize contemporary life amidst datafication – and what role anticipatory practices do in fact serve towards this goal. I explore this question in small ways throughout the thesis by demonstrating the many ways that security can be – and already is – reconfigured around values other than state and corporate constructs by civil society actors, pushing civil society security practices towards a notion of 'critical, disobedient anticipation' (Amsler and Facer, 2017:13). Even as I foreground civil society's work to reconfigure security, I also highlight moments in which there is more work to be done to align everyday data practices and strategies of surveillance resistance with an emancipatory politics capable of giving 'us' the room we need to pursue human rights and social justice in a time of crisis.

Finally, in studying the future-oriented dimensions of civil society responses to the uncertainties and harms of contemporary surveillance, I note that my research is not simply concerned with 'futures'. Rather, I continuously examine the tension between persistent problems and speculative concerns about possible future threats, looking at how this tension gives rise to particular orientations towards the future. I argue that keeping this multi-temporal grounding is important, considering how much attention has recently been placed both within academia and civil society on the risks of 'high' technologies, such as recent advancements with artificial intelligence. Even as debates rage on about the future of artificial intelligence systems and their promised imbrication into all

facets of life, many people at the front lines of human rights and social justice work remain busy with old but deeply entrenched problems tied to resource constraints and the labour of maintaining existing infrastructures. Such problems include not being able to afford trusted IT support, struggles with unreliable privacy enhancing technologies, and powerful and persistent adversaries that remain one step ahead even when 'sophisticated' measures are taken to defend against surveillance and profiling. Amidst this shifting landscape, civil society actors are effectively asked to balance immediate problems caused by persistent constraints with concern over the threatening promise of emerging technologies for surveillance. As advanced surveillance technologies increasingly become embedded into everyday infrastructures and data-driven technologies pervade everyday life, civil society actors wonder what strategies for privacy, security and autonomy will be effective in the coming years. My thesis hence endeavours to look behind and ahead, conceptualizing sticky, persistent problems and peripheral futures within a single topology.

Interdisciplinarity & contributions

My research approach emerged from the intersection of several overlapping fields concerned with the study of socio-political issues amidst rapid technological change. While developing the research approach for this thesis, I read from several different literatures dealing with social practices and technological change. These overlapping interdisciplinary fields together inform my approach to the study of resistant practices and infrastructures, which I expand in more detail in Chapter 2, which serves as my literature review chapter. For now, I only provide a summary.

First, the thesis builds on and directly responds to several decades of **surveillance studies** literature on resistance and counter-surveillance. The field of surveillance studies offers a rich body of empirical literature studying surveillance implementations and how communities have resisted them. This literature informs my theoretical understanding of the social dynamics between surveillant and resisting actors. I build on and contribute to this area of surveillance studies by shedding more light on the anticipatory dimensions of surveillance resistance and how the anticipatory dimension of resistant practices drives the 'dance of surveillance' and resistance (c.f. Marx, 2009). I also contribute to the fields' theorization of resistance by conceptualizing resistance as a productive force intrinsic to everyday safety-movement-building processes, rather than only serving as symbolic or aestheticized acts of dissent (as per Monahan, 2006; 2015).

Second, this thesis builds its theoretical and methodological core from **information studies and science and technology studies (STS)** literature concerned with sociotechnical practices, information infrastructures, and the politics therein. Feminist technoscience provides an incisive lens to understand how contestations amongst different social groups shape practice and infrastructure (c.f. Star, 1999; Suchman, 2002). Studies of valuation (c.f. Ballestero, 2015; Callon and Law, 2005) enable me to understand the calculative logics imbricated within the anticipatory practices enacted by civil society actors. I build on and contribute to this literature by shedding light on the importance of feminist epistemologies of security, and by building an understanding of how calculative risk logics emerge from intersubjective processes of valuation.

Third, the thesis draws from the field of **critical security studies** to examine how anticipatory logics generate particular political possibilities and cause foreclosures (c.f. Anderson, 2007; Amoore, 2013). This field of study offers a rich theoretical base for understanding risk and threat construction as socio-political processes. I apply the field's understanding of risk as a processual and intersubjective phenomenon towards my

empirical study of risks and threats in the context of digital security and resistant practices. I build on and contribute to this literature by applying its rich understanding of the anticipatory logics of state and corporate security actors towards a novel purpose: I take the study of anticipation beyond the state and corporate contexts and into civil society.

Finally, I draw on **critical data studies** for its situated examinations of data practices (c.f. Mackenzie, 2013; Pink et al., 2018;), which show a way to use the anticipatory dimensions of everyday data practices to build a bridge to the study of risk and threat construction. I build on and contribute to critical data studies by enriching the field's understanding of the anticipatory dimensions of data practice, feminist epistemologies of data and security, and the politics of data infrastructuring. By giving concerted attention to the struggles that come with dealing with surveillance and data-related uncertainties, I also contribute to the field's understanding of human agency in relation to societal processes of datafication. I particularly demonstrate how different social groups are fighting to break free of the hegemonic risk logics and anticipatory regimes of contemporary surveillance.

Structure of thesis and methods of data collection and analysis

This thesis takes shape in the form of a multi-sited ethnographic study of surveillance resistant practices and infrastructures. It draws on data collected from 50 semi-structured interviews, participant observation at 12 conferences and workshops in Europe and Southeast Asia, and the close reading of civil society texts on surveillance self-defence, digital security, and cybersecurity. The five core chapters of the thesis, starting from Chapter 4 to Chapter 8, are derived from a reflexive thematic analysis of the data. This method is based on an inductive approach to analysis that

surfaces themes from the data and facilitates inductive theory production, rather than already imposing theoretical frameworks onto the data in advance. I discuss my methods of data collection and analysis in more detail in Chapter 3, where I outline my research design.

Chapters 4-8 of the thesis were planned as five full-length scientific articles intended for submission into peer-reviewed journals, as part of an agreed format of 'thesis by publication'. That is why each of these chapters of the thesis conforms to approximately 8000 words in length. Two of these chapters of the thesis have already been published in peer-reviewed journals (Chapters 4 and 5) while the rest are under peer review. Across the thesis text they are referred to as chapters, though they are structured as articles. In the next section of the introduction, I introduce the main themes of the thesis and disciplinary positioning, before providing summaries of each of the core five chapters.

Central themes of the thesis

As mentioned, the structure and topics of this thesis emerges from a reflexive thematic analysis of data. In this section, I briefly summarize the main themes that emerged from my empirical analysis.

Anticipatory logics: The central theme of study in my thesis is the anticipatory logics that shape the work of responding to surveillance-related uncertainties, threats, and harms. In this thesis, I conceptualize anticipation as the future-oriented dimension of practices and infrastructures that resist surveillance. Under the umbrella of 'anticipation' I include varied state, commercial, and civil society practices shaped by logics of risk, preemption, prediction, prevention, and resilience, among others. While these anticipatory logics are distinct, they are also characterized by their conceptual slippage and mobility throughout different social realms. In my thesis, I trace the mobility and contextuality of anticipatory logics as they are appropriated and

reconfigured within civil society practices. Not only do I look at how civil society appropriates and reconfigures anticipatory logics through resistant practices, I also seek to understand how the anticipatory logics of state and corporate actors violently clash with those of civil society actors.

Anticipatory dimensions of resistant practices: As previously mentioned, in this thesis, I use anticipation as a lens through which to study the surveillance resistant practices of civil society. The practices I explore are framed by civil society as elements of digital security. I take a broad view of what digital security includes, understanding security as a heterogeneous field of practice which, in the daily life of people using technology, overlaps with issues of data privacy, data protection, corporate data exploitation, the harms of automated systems, disinformation, and counter-surveillance. I explicitly connect the study of digital security practices with surveillance resistance, understanding digital security as an effort to resist different contemporary forms of surveillance and mitigate its related harms.

The practices of concern in this thesis are different forms of threat modelling, risk assessment, and other explicitly anticipatory practices. These socio-material practices are structured to help people tame uncertainty and contend with probable future threats and harms. I focus on exploring the enactment of these practices in the context of broader processes, such as the infrastructuring of new collective threat response mechanisms (threat intelligence sharing platforms, rapid response help desks, and the development of new security standards and security threat taxonomies, as per Chapter 7); security trainings and surveillance-awareness-raising interventions (chapters 4, 6, & 8); feminist pedagogies of security (chapters 4, 6, & 7) and the development of new software to mitigate threats related to intrusions by state actors, IoT systems, and biometric surveillance (Chapter 5). As part of my study of practice, I attend to the affective, temporal, epistemological, and socio-material dimensions of anticipatory action involved in making sense of and responding to threats. For example, I explore a widely expressed

imperative by interviewed respondents to be 'proactive' in responding to surveillance threats. I look at how being proactive means taking up anticipatory modes of work to avoid undesirable surveillance futures (Chapter 8).

Finally, in this thesis I explore how anticipatory logics and practices emerge in relation to shifting **civil society priorities.** The priorities I explore throughout the five core chapters include:

- A desire by civil society actors to increase the efficiency of civil society threat response through collective mechanisms, data-driven techniques, formalized security standards, and the use of automated prediction.
- A perceived need to professionalize the different roles and responsibilities of technology and digital security-focused work.
- The struggle to increase the equity and diversity of experts and expertise (particularly their geographical, racial, socioeconomic, and gender diversity).
- The mainstreaming of feminist epistemologies into civil society digital security work.
- Questions about how to effectively address persistent problems of security and technology maintenance amidst the continuous emergence of new surveillance threats.
- Issues of epistemic justice arising from the inequities between rich organizations in the United States/Europe and groups in the Global South or 'majority world.'
- A (lack of) sustained funding and material resources for technological and movement building work against surveillance threats.

As I document throughout this thesis, all these priorities are subject to continued contestation. Hence, this thesis seeks to understand responses to threats in relation to the **tensions, controversies, and shifting problem**

definitions of civil society. The ones identified and documented throughout include:

- Tensions between civil society actors who emphasize the importance of self-defensive security tactics versus those that emphasize advocacy to change technologies and regulations.
- The push for the articulation of a movement-level politics of data versus a focus on developing tool-driven technology 'fixes'.
- Tensions around the scale and geographical configuration of work between organizations, namely global and transnational versus local and trans-local.
- The merits of qualitative versus quantitative approaches to managing risk.
- The advantages and disadvantages of centralized versus decentralized security infrastructures.
- Tensions between universalist and contingent/contextualized understandings of surveillance and surveillance resistance.
- Tensions between reform versus abolition-oriented strategies of resistance and advocacy.
- Tensions around belonging to civil society versus belonging to 'movements' or 'communities', and relatedly, tensions between human rights and social justice frames.
- Tensions between digital security and cybersecurity as overlapping yet distinct fields.
- Tensions around focusing on fixing persistent current problems versus raising awareness of speculative, emerging concerns.

Having briefly introduced the themes of this thesis, I next provide an overview of its five core chapters.

Thesis Chapters overview

I conclude this chapter with a summary of the five chapters that form the core of this thesis. To remind the reader, the primary question explored in my thesis concerns how **transnational civil society grapples with the uncertainties of contemporary surveillance-related threats and harms.** My broader goal in asking this question is to build an understanding of the logics, practices, and infrastructures that make acting amidst the uncertainties of surveillance and datafication possible. I explore this question throughout the five chapters that emerge from a reflexive thematic analysis of my empirical data.

Chapter 4 tackles the challenge of finding any sort of 'solution' to harms experienced from contemporary surveillance concerns. It is titled "It depends on your threat model: Understanding the anticipatory dimensions of resistance to data-driven surveillance" and was published in *Big Data & Society* in January 2021. This chapter explores how digital security practitioners, human rights defenders, and the movements they work with together try to untangle the complexities and uncertainties of data exploitation and surveillance through threat modelling and risk assessment practices. In the chapter, I explore threat modelling and risk assessment as 'anticipatory data practices': future-oriented data practices which 'tame' uncertainty and aid people concerned with digital surveillance and data 'mess' to understand how to respond to their threats. Throughout the chapter, I explore the significance and varied configuration of anticipatory data practices in the context of broader shifts in civil society practice over the years it has increasingly engaged in mobilizations against digital surveillance. The main shift I document here is not in the 'tools' to counter surveillance but in what it takes to cope with the totalizing overwhelm that comes with determining how to act under duress of potential threats and harms. I explore both what

emancipatory possibilities anticipatory data practices open up, as well as the sorts of political foreclosures they may enact.

Chapter 5 is titled “Bodies not templates”: Contesting Dominant Algorithmic Imaginaries and has been published in *New Media & Society* in January 2021 with co-author Stefania Milan. This chapter comprises a study of three open source software projects produced by civil society actors who try to address some of the many harms of contemporary surveillance and datafication. The study of these three projects is intended to provide a way to understand changes in the concerns and problem definitions of security specialists, software developers, digital security trainers, and affected communities, in relation to a landscape of shifting digital threats and a shifting attention economy. Together with co-author Stefania Milan, we propose a heuristic for understanding how certain action repertories within civil society emerge and become stabilized, only to break and shift once more in response to changed technologies and political concerns. Part of a special issue on sociotechnical imaginaries, the chapter focuses on identifying the ‘counter-imaginaries’ at play in the development of three open source software projects dealing with threats arising from targeted surveillance of personal devices, data exploitation of the Internet of Things, and automated (artificial intelligence-driven) face surveillance. The chapter exposes the contradictory values and logics at play within these technological projects, contributing to an interdisciplinary understanding of how different social groups make sense of the challenges of datafication from the ‘bottom-up’. The chapter also tries to offer a novel lens for understanding sociotechnical change.

While Chapter 4 surveys anticipatory data practices in the context of civil society digital security, in Chapter 6, I look in more depth into the enactment of risk assessment, exploring it within the particular context of ta digital security training organized for human rights defenders. Titled: Taming uncertainty into risk: towards a critical lens on risk management practices in digital and cyber security’, this chapter introduces the concept

of ‘qualculative convergence’ to describe the intersubjective process that transforms unwieldy uncertainty into formalised digital security risk. With this concept, I make a critical intervention into enterprise risk and security tropes, challenging rationalist and behaviouralist discourses common for commercial and state cybersecurity by demonstrating the ‘messy’ forms of collective valuation that go into the construction of a risk as such. Through this ethnographic exploration of a digital security training, I show how digital security trainings facilitate the transformation of uncertainty into risk, and how the training culminates in convergence around an appropriate path of action to counter surveillance and digital harms.

While Chapter 4 and 6 focus on understanding the imbrication of anticipatory modes within practices of risk assessment and threat modelling, Chapter 7 looks at the role of anticipatory practices in the *infrastructuring* of online platforms designed to allow people from different communities of security practice to collectively anticipate threats. Titled ‘Infrastructuring the future(s) of cybersecurity: towards fully-automated anticipation?’, the chapter looks at the emergence of what I term 'anticipatory security infrastructures': information infrastructures shared between different communities of security practices, which are intended to facilitate the collective anticipation of security threats. The chapter investigates the politics of data standards and threat taxonomies that are involved in their infrastructuring. In the chapter, I show how these anticipatory infrastructures bring commercial and state cybersecurity actors with NGO workers and digital security experts together across diffuse configurations to collect, analyse, and track data towards the goal of anticipating and preventing damaging future surveillance-related events. The chapter identifies and analyses two contrasting approaches to infrastructural anticipation, one premised on increased centralization and the application of data-driven and automated processes and another that foregrounds autonomous, local, and feminist approaches to data and security.

My final empirical chapter, Chapter 8, is titled "Preventing Preemption: exploring proactive strategies to counter anticipatory surveillance regimes". This chapter documents an imperative among human rights defenders and social justice movements to act 'proactively' in anticipation of preemptive surveillance and policing measures. I conceptualize proactivity as an anticipatory orientation geared towards the avoidance of violently preemptive actions against human rights defenders and social justice movements. I devote a separate chapter to examining the notion of proactivity because the concept had thematic importance among respondents interviewed for the thesis, who expressed the need to be 'proactive' rather than 'reactive'. The chapter consists of two cases through which proactivity is explored. The first case looks at proactivity as it is negotiated in a digital security training, while the second case explores a conversation led by a grassroots group of abolitionist organizers working to dismantle predictive policing programs and data-driven discrimination in the United States.

Conclusion

This chapter has introduced my research puzzle, research inspirations, and research questions. Further, I summarized the central themes of the thesis, as well as my disciplinary influences and contributions to several different fields of study. Finally, I provided short descriptions of each of the five core chapters of the thesis. In the next chapter, I situate my research questions in relation to the different disciplines I engage with.