What harms may come?

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

Kazansky, B.

Publication date
2021

Chapter 2. Literatures in conversation on resistance, anticipation, practice, and infrastructure

Aims, literatures, and focus

This chapter sets up the framework for my study of resistance to contemporary surveillance by reviewing and synthesizing relevant literatures. In Chapter 1 I introduced my thesis, which draws on several interdisciplinary fields: surveillance studies, science and technology studies, critical security studies and critical data studies. As this literature review chapter cannot begin to fully account for the rich genealogies of all the fields listed above, I focus on how their intersections elucidate the main themes of my study of anticipation, security, civil society, data practices, and infrastructures. The plan for the literature review is as follows: I first discuss how resistance is conceptualized in the field of surveillance studies, looking at the main debates and positioning this thesis in relation to them. I then expand my discussion of resistance further by examining fields and disciplines concerned with the study of data practices and security, including information studies, privacy engineering, and critical data studies. Next, I come to my particular focus on how people make sense of uncertainty through anticipatory modes and practices, contextualising these concerns in relation to critical security studies. Finally, I discuss how feminist technoscience informs my research approach, particularly in how I investigate practices and their relationship to information infrastructures.

What counts as resistance? Civil society as a countervailing force

What kinds of practices qualify as resistance to surveillance? This question pervades literatures concerned with agency, technology use, and social movements. It also comes to bear on my thesis, which closely examines surveillance resistant practices that are often grouped under concerns with digital security and cybersecurity. Resistance to surveillance can be conceptualized at different registers, which scholars have tried to organize through taxonomies and comparative analyses of tactics and strategies (Martin et al., 2009; Marx, 2009; Monanhan, 2006; 2015). Surveillance scholars have argued that though resistance is 'a central theme in surveillance literature... [yet] as a concept, remains undertheorized' (Fernandez and Huey, 2009: 200). Fernandez and Huey attribute this under-theorization to the 'generalized nature of the concept, which can cover over vast territories of divergent action' (200). Martin et al., (2009) concur, arguing that 'the concept has yet to receive a thorough, systematic and focused elaboration in the academic literature' (2009: 214). However, rather than try to nail down a rigid definition, they push for a refocusing. They argue for 'an understanding that resistance too [just as different forms and manifestations of surveillance] will be contextual, relational, and dependent on the power dynamics of a given situation'.

Martin et al.'s critique was spurred by their observation that surveillance studies research trained a narrow lens on antagonistic relationships between 'surveyors' and the 'surveilled', as exemplified in the dynamic of opposition between activists and governments. 'To simply equate resistance with public protest is to severely understate what resistance is all about, who participates and how' (214). This narrow framing of resistance has the effect of 'neglecting other possible actors who resist surveillance processes in various ways' (214), such as 'NGOs, civil society and industry, and technology as actors bound up in resistance to

surveillance' (229). They thus argue for the expansion of the scope of analysis to account for the social complexity of contemporary surveillant assemblages: 'though surely important, the relationship between a domineering government and a hapless citizenry is but one part of what must be a more complex, multi-directional and multi-actor resistance process' (214). It is fair to say that a decade after Martin et al.'s proposal for an expanded research agenda on resistance, much of it has come to fruition. Their urging to expand the lens of analysis beyond simple oppositional dialectics resonates with David Lyon's desire to look beyond the monolithic 'surveillance society' to instead examine an ecology of different surveillance cultures, practices, and imaginaries, which interact and refract in different ways (2017). In Lyon's reading of culture, institutions and individuals are all understood to navigate a life suffused with surveillant logics. Novel forms of 'lateral surveillance' and 'digilantism' (Andrejevic, 2005; Mols and Pridemore, 2019; Trottier, 2017) reconfigure the day-to-day relationships between powerful actors and citizens, enacting new delegations of power and responsibility. Lyon thus urges more attention to practices and imaginaries, a call I take up in my thesis. Indeed, practices, infrastructures, and (at some points) imaginaries are the locus of my study, allowing me to trace how particular logics and rationalities driving increased surveillance 'travel' and take hold of populations and groups.

As for the urging by Martin et al. to direct more attention to the activities of civil society, an enormous amount of literature has emerged (in fact, long before their 2009 article, and not just within the field of surveillance studies itself) to document and critique advocacy campaigns (Bennet, 2008), hacking cultures (Coleman 2010; Dunbar-Hester, 2013; Kelty, 2008), and grassroots movements (Milan, 2013). The leaks of Edward Snowden in 2013 served as a scholarly and public reckoning that confirmed theoretical and empirical concerns about state surveillance regimes. These 'revelations' led to much debate, both in terms of what they revealed about suspected surveillance and the implications for how to

counter it from the perspective of protective technologies and social mobilizations (Bauman et al. 2014; Lyon, 2015). The start of the DATACTIVE project[1], which also brought about this thesis, came on the crest of this 'post-Snowden' moment, at the same time that an increased attention to 'big data' was forming a new locus of interdisciplinary attention. Studies of data activism trained a lens on how organized civil society uses data, both to resist the expanded forms of data collected across society and to mobilize this data towards different ends (Milan 2016; Milan and van der Velden, 2016). At the same time, the urgent activities of tech actors and public interest groups in support of surveillance accountability and new encryption technologies became a subject of critique for scholars concerned with the politics of civil society work, training their eyes on the unexamined ideologies and power structures of the field. These contributions highlighted the contradictions of counter-surveillance activist 'elites', who in their push for transparency and reform, also propelled a technocratic vision of resistance (Gürses et al, 2016). Aouragh et al. (2015) critiqued the 'sneaky moments' that reinstall the very power dynamics of concern. Dencik et al. (2016) drew attention to the lack of uptake of surveillance issues in broader social movements.

Between 2013 and 2015 I myself engaged in a 'proximal critique' of these issues, from my position in civil society as an action-oriented researcher and practitioner. At the time, I was tasked with a research project which sought to unpack why civil society's digital literacy and surveillance

1 The DATACTIVE project was a research project funded by a Starting Grant from the European Research Council from September 2015-June 2021 to study the 'politics of big data according to civil society.' The Principle Investigator was Stefania Milan, at the University of Amsterdam. I was hired into the DATACTIVE project as as PhD researcher in 2015 to focus on how 'citizens resist data collection'. My individual thesis emerges in relation to the larger DATACTIVE project and its questions.

education efforts were failing to meet their stated goal to support human rights defenders in dangerous situations. My research was confined to the arena of human rights defenders' technology adoption and 'digital security trainings'–a form of intervention that became increasingly common across Internet freedom and digital rights organizations attempting to foster the adoption of 'secure practices' at the grassroots level. The main findings of this research were that the desire to 'change behaviours' among affected populations threatened to perpetuate a program of neoliberal self-management amongst people facing harm. As the specifications of the project required me to also offer constructive ways forward, my recommendations focused on ensuring that strategies for privacy and security 'support' were responsive to the lived experience of different groups, and that emphasis was put on ensuring that these strategies were supportive of collective action (Kazansky 2015; 2016). My findings provided empirical confirmation to legal scholarship emerging around the idea of 'group privacy', which argued for privacy to be reframed separate from an individual right to a social good (Taylor et al., 2017).

An interesting moment of self-reflection followed when 'data justice' emerged as a proposed framework through which to build inter-movement solidarity on technology-related social justice issues (Dencik et al., 2016). At the time, Dencik, the Data Justice Lab and members of the European Research Council-funded Data Justice Project at Cardiff University took steps to reframe the issues at stake away from surveillance, tech activism, and privacy to one of 'data justice' – a constructive framework that foregrounds the political and collective dimensions of data across society (Dencik et al., 2016). Findings from my practitioner research were cited in the early work of the Data Justice Lab as evidence that the efforts made by technology-focused activists to spread public awareness of the threats of surveillance through technical interventions had failed to reach the communities most directly targeted. Hence, the Data Justice Lab advocated for more solidarity across different social movements in its

work. I found myself in wholehearted agreement with these conclusions. Yet, by this point in my PhD, my early fieldwork had shown ample signs that civil society itself was engaged in a reflexive process of learning from the frictions and failings highlighted by the Lab – a phenomena that I chronicle throughout my thesis. The special issue in *Krisis Journal* on data activism in 2018 (Milan and van der Velden, 2018) brought critiques about the exclusions and frictions highlighted above to the study of 'data activism' (Milan, 2016). In the issue, Horgan and Dourish (2018) examined civil society activism as a diverse and fractured field of action, building on Chantal Mouffe's argument that 'politics always takes place in a field criss-crossed by antagonisms' (236: 2013). In the same issue, Helen Kennedy argued for more study of everyday data practices rather than just explicitly 'Political' ones. In so doing, she argued that scholars of critical data studies should attune themselves also to the 'small p politics' of practices and infrastructures (2018). In my thesis, the political differences and movement fractures pointed out by Dencik and co-authors and Horgan and Dourish suffuse my fieldwork data, and enrich my understanding of the contestations within and around civil society –a subject integral to my study. My study also focuses on the exploration of practices and infrastructures, thereby attending to the 'small p politics' bound up in them.

The ambivalence of resistance as concept and phenomena across disciplines and fields concerned with technology and society

There have been a few moments during the thesis when I questioned whether the term 'resistance' adequately captured the subject of my study. As I have alluded to above, what constitutes resistance to surveillance is a subject of perennial debate. As technologies, politics, and social dynamics

change, so do modes of resistance. Further, depending on the context of its formulation, resistance may be contrasted with other modes of action in response to social issues. Whether a form of action is considered resistance is contextually in flux as particular politics become dominant and 'new' technologies are integrated into the fabric of daily life (c.f. Martin, et al., 2009). Studies of pushback to surveillant processes and institutions across different literatures demonstrate the heterogeneity of terms and definitions around resistant counter-practices and social dynamics. These practices may be discussed in terms of digital and grassroots activism (Dunbar-Hester, 2013; Milan, 2013; West, 2017); 'counter surveillance' (Mann, 2002; van der Velden, 2018), 'anti-surveillance activism' (Dencik and Cable 2017; Gürses, et al., 2016), digital/cyber/IT security (Ermoshina and Musiani, 2018; Kazansky 2015; 2016; Notley and Hankey, 2013; the Citizen Lab, 2014; Zajko, 2018); privacy (Nissenbaum, 2010; Taylor, et al., 2017), digital/data literacy (Brand and Sander, 2020; Carmi, et al, 2020; D'ignazio, 2017), data feminism (D'Ignazio and Klein, 2020); data activism (Milan, 2016; Milan and van der Velden, 2016) or refusal (Benjamin, 2016; Gangadharan, 2020). 'Resistance' may refer to symbolic, isolated acts of dissent (per Monahan, 2006), or transformative, long-term pushback against dominant narratives, imaginaries, infrastructures, and regimes of surveillance – such as in abolitionist research/action groups like the STOPLAPD Spying Coalition (StopLAPD Spying Coalition, 2018) and Critical Resistance (Critical Resistance, 2021).

Much work on what could be called resistant practices has taken place outside of studies of civil society and social movements. The phenomena under study do not always get classified as resistance. For example, while a digital security practice such as the encryption of email might be considered a practice that is 'resistant' to surveillance or feeds into broader strategies of resistance amongst civil society and social movement actors (c.f. Zajko, 2018) it is more often conceptualized as a banal, daily element of information management across societal realms and

organizational contexts. Conversations about practices that block, avoid, or mitigate the harms of surveillance and related digital threats have been advanced through the study of information security, computer security, and cybersecurity (Dourish et al., 2004; Dwyer, 2019; Slayton, 2015; 2020), hacking (Coleman, 2013; Dunbar-Hester, 2019; Kelty, 2008; Tanzer 2016; 2020), and privacy-enhancing technologies (Gurses, 2010; 2011; 2016). The related yet distinct fields of human-computer interaction (HCI), information studies, and critical data studies have revealed just how many different and creative tactics are created by people across disparate contexts to cope with the everyday 'mess' that accompanies life in a datafied society (Pink et al., 2018). People strategically choose to disclose or not disclose information in ways that work around the contextual particularities of online communities and platforms (Marwick and boyd, 2014; Nissenbaum, 2010); save and duplicate important information by backing it up on devices and cloud services (Pink et al., 2018); engage in 'vernacular resistance' through the use of codewords (Brunton and Nissenbaum, 2015; Gaw and Felten, 2006); temporarily disable social media accounts (boyd, 2008), or choose to entirely avoid the use of particular technologies (Baumer et al., 2015; Eubanks, 2011; Satchell and Dourish, 2009;Wyatt, 2003).

Meanwhile, computer scientists, engineers, and hackers continue to develop new technologies and infrastructures against an ever-shifting milieu of threats and vulnerabilities. Amidst AI hype cycles and documented AI harms, the burgeoning Fairness Accountability and Transparency community of data science-focused scholars develop frameworks to test 'fairness' and de-bias the datasets used in automated decision-making systems (Rhagavan et al., 2020). Its more subversive members brainstorm how to subvert the logics of optimization that guide the actions and outcomes of machine learning logics and data-driven platforms and infrastructures (Gürses et al., 2018). This field is now moving on from technical questions of bias in data sets and algorithms to consider how technical bias is an artefact of racist and discriminatory

processes across society and within data science itself, pushed towards introspection by anti-racist scholarship of technology and society, including the work of Benjamin (2019), Buolamwini and Gebru (2018); Gangadharan and Nicklas (2019) and Noble (2018). By showing that contemporary issues related to automated systems are part of a continuum of historical oppression, anti-racist scholars of technology and society bring abstract discussions around bias in technology back to the concrete concerns and lived realities of targeted communities and social movements fighting for social justice and human rights. As they do so, it is evident that issues around everyday safety and security remain a persistent concern for these communities and movements. In light of the continued importance of safety and security practices, my thesis attends to the ongoing 'small p politics' of everyday security and data practices and their role in the 'big P politics' of movement building, policy, and the fight against discriminatory systems.

I have previously documented that the challenging pursuit of safety and security has become imbricated into the daily work of human rights defenders (Kazansky, 2015; 2016). Indeed, the number of campaigns against particular groups and individuals over the years (Citizen lab, 2014) has contributed to a need to continuously update practice (Kaun and Treré, 2018). Despite the breadth and depth of work done to block or mitigate the harms of digital surveillance and digital threats, the question of which tactics and strategies are indeed 'effective' remains a subject of continued controversy (Aouragh et al, 2015; Dencik and Cable, 2017; Gürses et al, 2016; Monahan, 2006; Musiani and Ermoshina, 2017). As acknowledged by Brunton and Nissenbaum (2015), tactics and strategies for resistance to surveillance, digital insecurities and privacy infringements are not always successful, and even settling on a definition of success is elusive.

Amidst the deliberate opacities of data-driven institutions (Smith, 2018) and the constraints of commercial platforms and infrastructures (Van Dijk et al, 2018), it remains a perennial challenge to determine exactly how

individuals and communities can perceive, block, subvert, and avoid surveillance. Those who apply different tactics and strategies might only learn of their failure following dire consequences such as arrests, persecution, or worse. Meanwhile, success may go undetected. 'Success' against surveillance and related digital threats might entail simply being able to survive and continue one's work. In the absence of concrete evidence of digital compromise, monitoring, tracking and surveillance, countermeasures may only provide a 'simulation of safety', argues Hong (2015: pp.70). On the other hand, the sheer number of emergent sociotechnical practices challenge the notion of a society resigned to the matter-of-factness of continuous data collection and monitoring, as captured in the notion of 'digital resignation' by Draper and Turow (2019). For historically targeted groups and populations, the high stakes of surveillance 'discovery' (Marx, 2009) mean that despite any feelings of resignation, activities to counter or mitigate digital surveillance and related digital threats continue to be a matter of concrete safety.

Beyond tactics and strategies of everyday safety, the spirit of surveillance resistance today is embodied in several domains concerned with intersecting issues such as migration, automated systems, and social justice. The #techwontbuildit hashtag, created to counter the actions of the US Immigration and Enforcement Agency, and a growing number of actions taken in the name of tech workers' resistance (Tarnoff, 2020) reflect an awakening by workers within tech companies to the power of collective demands. Centuries of abolitionist, anti-racist work to challenge the carceral state have also been brought to bear against 'smart' policing mechanisms and other technologically related harms (Benjamin, 2019; Datafication and Community Activism workshop, 2019; Wang, 2018), carrying forward the work of scholars such as Ruth Wilson Gilmore (2007) and Angela Davis and colleagues (Davis and Mendieta, 2005). Efforts to ban and dismantle facial recognition systems across several cities in the US and the EU have raised hopes among many that 'big tech' might be strongly regulated, while exposing a simmering tension between

policy ‘reformists’ and abolitionists. Where reformists are seen to push for temporary bans – or ‘moratoria’ (Crawford, 2019) – on technology and engage in high-level multi-stakeholder policy arenas, abolitionist groups refuse to take a seat at such tables, seeing the dynamic as inherently unjust against the backdrop of countless lost Black, Brown, and immigrant lives. For these groups, there is no time to be lost on incremental reformist initiatives that not only fall short of broad structural change in the present, but risk diverting energy and attention away for good. The tension between reform and abolition exemplifies that ‘the labor of resistance may be divided among those who push for change from the inside, from the outside, and from the margin, each effort being essential to the others and to an overall movement of change’ (Meyerson and Scully (1995: 598, as quoted in Horgan and Dourish (2018)). The tensions between reform and abolition also highlight once more that civil society – conceptualized in this thesis as the realm beyond the state and corporations concerned with countering technologically mediated harms – is a fractured field (c.f. Amoore and Longley, 2008).

Among all these contested delimitations and ambiguities imbued with meaning(s) of resistance, I choose to advance resistance as a framing for the different kinds of security, risk, and data-related practices explored in this thesis for several reasons. First, an analytic of resistance is broad enough to encompass the heterogeneity of tactics and strategies that come into play in the day-to-day civil society activities of study. Second, it allows me to maintain a connection to the rich body of surveillance studies literature concerned with how power is challenged and harms are addressed through resistance. However, I make several interventions into how ‘resistance’ is conceptualized, responding to recent debates in surveillance studies, which have argued that some modes of resistance to surveillance are either limited in their ability to push back against social processes or in fact productive of more surveillance. Among those who critique resistance tactics on this basis is surveillance studies scholar Torin Monahan (2006; 2015), who points to the activist sabotage of

CCTV cameras to argue that much resistance to surveillance stays in the symbolic realm. Monahan's overriding concern is with the way that aestheticized resistance or symbolic resistance can reproduce surveillant logics, eliciting a persistent tension around whether tactics of resistance result in the cultural reproduction of undesired structures (and if so, what paths of action might take us beyond them).

This is also a question I take up in the thesis. However, the modes of resistance that form the focus of this thesis should not be understood as isolated, symbolic acts of dissent, but a part of broader efforts at movement building, immediate survival, and physical safety. Nonetheless, resistance is indeed productive, and in my thesis, I explore how certain productive logics are inscribed within practices and infrastructures of resistance. As I mentioned above, resistance does not have to refer only to individual tactics and symbolic acts – though this is how it is often conceived in surveillance studies literature. Resistance can also be understood as a productive force in the development of new imaginaries, new infrastructures, and new practices. In this sense, I follow those who have turned to the Foucaudian notion of resistance as a productive force (Pickett, 1996), from which follows the concept of 'productive resistance' (Ettlinger, 2018). Where resistance is conceptualized as refusal (Benjamin, 2016; Gangadharan, 2020), it embraces the emancipatory potential of a history of thought on the abolition of technology – and the Luddist idea that certain technologies do not necessarily have to exist. I use the term resistance to talk about forms of negotiation and contestation that result in new practices and infrastructures that challenge dominant imaginaries, structures, and regimes.

Starting from Resistance

In the previous sections I mentioned the call by Fernandez and Huey (2009) to focus more explicitly on the study of resistance. Here I wish to highlight one of their concrete proposals, which was to flip the usual genre in surveillance studies by starting scholarly investigations from the point of resistance strategies rather than the systems of oppression (surveillance included). They argue that this reorientation makes conceptual sense, because, per Hardt and Negri (2004), 'revolt is generally the innovator, with the state adapting and developing new forms of control to address the innovations' (200). I argue that there is an additional reason to start from resistance. In my reading across literatures related to surveillance and technological harms, I have observed that subject of resistance often arrives well into the text, sometimes even in the last chapter or paragraph, where it is positioned as the subject for future research. What explains this tendency? Likely it can be attributed to the demands of first documenting and analysing the inner workings of the surveillance system(s) of concern. Downplaying resistance may also occur due to an abundance of caution by researchers worried about disclosing actions that might make sensitive matters too legible to the State or corporate gazes (Hintz and Milan, 2010). There are indeed many valid ethical concerns regarding what it means to study the impacts of surveillance and how they are countervailed. I discuss these in depth in my research design chapter.

I would like to highlight that while I take up Hardt and Negri's call to start from resistance, I do not start from resistance simply for the sake of its innovative or novel aspects. As scholars have warned, the study of surveillance resistance risks being fetishized or aestheticised when scholarly focus is placed on showcasing novel tactics, particularly when they are understood to be individualized and dependent on a single person's skills and privileged access to particular technologies. As already

mentioned, Monahan has repeatedly pointed to this tendency (2006; 2015) in his examination of artistic projects and symbolic acts of dissent such as the sabotage of CCTV cameras. In 2019, Zeynep Tufekci warned of the dangers of discourse that reifies resistance as novelty in relation to media coverage of emerging mobilization tactics coming from the Hong Kong protests against the Chinese extradition bill (Tufekci, 2019). At one of the many crests of this movement's activities, Western media outlets wrote breathlessly optimistic stories about the unique collectivity of protestors and their 'sophisticated' tactics. These tactics included the use of umbrellas to hide from the torrents of teargas shot by local police; the highly organized assembly lines of food and medical triage; the use of lasers to confuse drones; and efforts to physically destroy the many facial recognition cameras set up across the island. At this heightened moment, several different Twitter accounts run by security specialists observing events from afar began to propagate a webpage collecting these different tactics. The webpage was quickly criticized by Hong Kong residents for mischaracterising and sensationalizing particular tactics and actions, therefore promoting inappropriate security countermeasures. Meanwhile, the protesters struggled to achieve substantive international support for their demands. This dilemma exemplifies a question I return to throughout my thesis: how can we as scholars and practitioners highlight agency and counter-power without fetishizing or de-historicizing particular resistance efforts? How might we properly contextualize individual agency to structural oppression and its effects on rights and justice?

Though my empirical data does not explicitly engage with this era of Hong Kong activism, I take up critical concerns with resistance novelty on two levels. First, I incorporate these critical concerns into my analysis of resistance strategies, framing resistant practices not as objects of fascination or symbolic acts (c.f. Monahan, 2006; 2015), but as necessary expressions of agency resulting from a harmful societal dynamic. Second, I bring critical concerns around resistance to the research sites I study, by attending to social frictions as they arise within the countervailing

activities of transnational civil society actors working on issues related to Internet freedom, digital rights, and digital security. This is not to say that the forms of resistance I look at are not generative of exciting new possibilities for agency and counter-power, only that the 'novelty' is, in itself, not my primary concern. Considering that my research looks at actions taken for safety in often explicitly contentious or dangerous circumstances, I strongly agree with critics of the Hong Kong coverage that it would be a mistake to celebrate novelty that comes at the cost of lives, trauma, and disruption of movements. Yet, despite the problematics of resistance studies, as outlined above, I argue that the most important justification for centring the study of resistance is to document that despite the harms caused by particular systems of social control, agency remains a part of daily experience.

Relatedly, I argue that there is an essential value to foregrounding alternative epistemologies and imaginaries (or as Stefania Milan and I call them, 'counter-imaginaries' in Chapter 5) in order to challenge the idea that surveillance and datafication harms are inevitable facts of contemporary social life. I make this argument in response to the deterministic aura of inevitability that has coalesced around the AI-driven dystopias that have been both warned about and reified by powerful corporations and commercial actors. This deterministic vision of technology and society also finds its way into social science and computer science studies of people's 'behaviours', which have often been explained through the financialized logics of incentives and trade-offs (Acquisti, 2010); racist pseudoscientific instruments such as phrenology and its contemporary versions in facial and emotion recognition (Stark and Hoey, 2021); and a growing milieu of predictive AI-driven instruments developed in the name of progress and innovation by corporations. Even nuanced studies of attitudes towards surveillance may ascribe a degree of deterministic resignation to the idea of a society that pervasively surveils its subjects (see: Draper and Turow, 2019's notion of 'digital resignation').

Amidst the determinism and pessimism that surrounds human agency and counter-power in the face of high technologies, it is no doubt crucial to continue to document the onslaught of new technological systems and their harms. However, I argue that it light of pervasive imaginaries of resignation and technological determinism, it is at least as important to highlight the breakages, empty hype, and daily contestations that show the cracks in the wall, so to speak. Challenging the idea that technologies and systems are inevitable results of technological progress is essential for technology scholars and movements engaged in countering technological harms, as I and many of the people interviewed in this thesis argue. To meaningfully, constructively, and ethically study surveillance resistance, I therefore argue, is to recognize and study the indeterminacy of (social)life. Just as I highlight the continued persistence of resistant practices in the face of technological threats, I also underscore the many ways that practices of resistance do not conform to ideologically pure distinctions between work done within and outside of hegemonic systems. There are a number of ambiguities involved in working towards human rights and social justice while also being subjected to the constraints and closures of our contemporary socio-political and economic contexts (Amoore and Langley, 2004; Dunbar-Hester, 2013; van der Velden, 2018). These ambiguities mean that people may engage in resistance while also experiencing feelings of resignation. They may use commercial platforms while decrying those platform's policies, and they may apply hegemonic risk logics to their work in order to assess their risk of danger, while also fighting to end institutional risk profiling. These ambiguities are highlighted throughout my thesis, as I explore how different anticipatory, future-oriented logics that come into play for people trying to avoid undesirable futures involve both the appropriation and re-configuration of hegemonic conceptualizations of risk and security. In the next section I further discuss my approach to understanding the role of future-oriented logics in the study of resistance.

From uncertainty to anticipation

At the start of my thesis in 2015, I anticipated rapid changes to civil society as a 'field' and in scholarly debates around technology and society. For this reason, I sought to anchor my thesis in a persistent object of concern in scholarly and practitioner work. Specifically, I wanted to study the struggle within civil society to break the uncertainties of pervasive yet evasive surveillance into something that can be understood and dealt with on a daily basis. My concern crystallized around the notion of what I call 'surveillance uncertainties' – a nagging problem for civil society actors engaged in education and support of practical countermeasures against surveillance. The discussion about uncertainty often came up in settings mediated by technical security specialists in discussion with frontline groups. who would come searching for concrete solutions to the problem their communications might be monitored by states wanting to disrupt their work. They would ask experts what 'tool' would be best to deal with the problem. The expert in turn would answer: 'it depends on your threat model'. The pervasiveness of the threat model as a conversational anchor and a frame for managing uncertainty seemed significant to me. In my thesis, the study of threat modelling becomes a way to trace the movement of a practice as it is appropriated and reconfigured across the work of technology developers, engineers, computer scientists, human rights defenders, social justice activists, and NGOs. While this tracing seems to stretch across a very broad selection of actors and distinct 'communities of practice' (Lave and Wenger, 1991), I focus on studying their points of interaction in specific contexts, such as emerging security infrastructures built and maintained by multiple communities of practice responding to the threats of surveillance. The exploration of meeting points also offers a chance to study the agonistic or contentious politics that Mouffe points to as an object of study (explored in the context of data activism by Horgan and Dourish, 2018 and Beraldo and Milan, 2019).

Whereas my thesis began with a goal to understand how uncertainty is grappled with, my first fieldwork findings highlighted the importance of 'anticipatory modes' (Pink et al., 2018) in breaking down or 'taming' uncertainty. Through my research, I found that for security specialists collaborating with NGOs and grassroots groups, the process of making sense of surveillance uncertainties involved a repertoire of practices focused on anticipating future harms. Of particular concern to me are the 'anticipatory logics' (Anderson 2007; 2010) that suffuse everyday life amidst datafication (MacKenzie, 2013), which become inscribed within the resistant practices of threat modelling and risk assessment, and give shape to sociotechnical infrastructures (Clarke, 2015). In my thesis, I tie the productive qualities of resistance (c.f. Ettlinger, 2018; Monahan, 2006) to its future-focused, anticipatory dimensions, the intwining of which becomes a central theme of my study of how civil society contends with uncertainties and opacities of datafication.

One of the main early findings in my fieldwork is that to mobilize and respond to the harms of contemporary surveillance, targeted communities working with technologists and security specialists have increasingly turned to anticipatory modes of work to prepare for and mitigate probable future harms. My thesis thus became focused on the study of 'anticipatory modes' (c.f. Pink et al. 2018) of resistant practices, which I explore by conceptualizing 'anticipatory data practices' (Chapter 4) and 'anticipatory security infrastructures' (Chapter 7) that arise in efforts to resist surveillance-related threats and mitigate their harms. There are a number of questions to ask about what it means, from the perspective of agency, politics, and power, to become 'enrolled' in anticipatory logics and regimes. Drawing on Adrien Mackenzie's work (2013), I ask how the need to anticipate future harms creates new forms of labour and responsibilities for front-line actors. Drawing upon Massumi's critical theories of preemption (2015) and Amoore's explorations of 'possibilistic' risk (2013) and the ethico-political dimensions of algorithms (2020), I ask how the productive force of anticipation in the

context of resistant practices might foreclose futures and diminish the space to imagine and enact emancipatory politics.

I note that in many cases, the people I interviewed did not explicitly frame their concerns and work around anticipation. They often spoke instead of risks and threats, and the need to take predictive, proactive, preventative, and 'preemptive' measures in response. My fieldwork showed these terms were often used in variable and sometimes interchangeable ways to discuss their overarching desire to avoid undesirable futures. The interchangeability of future-focused logics in the lexicon of civil society parallels a definitional confusion I have encountered in academic literatures related to the study of national security, cybersecurity, intelligence, and policing. This definitional confusion indicates a conceptual slippage between anticipatory logics, which in itself is a central subject of study. One example of this definitional confusion can be found in academic and police discourse on predictive policing. While the term predictive policing obviously contains the world *'predictive'* and is often discussed as such within the data sciences, critical scholars of data, policing, and security demonstrate that these policing systems and techniques are in fact *preemptive* (Massumi, 2015; Andrejevic et al, 2019; Andrejevic, 2020; Williams, 2019). Why make the distinction? While the prediction in predictive policing refers to the predictive data analytics in use (such as Palantir's data-driven platforms and analytics dashboards), focusing on these predictive analytics in isolation can miss the bigger picture. When zooming out to consider the productive effects of predictive analytics and the overall goals of these systems in historical contexts, it becomes clear that predictive analytics are simply the contemporary instruments of longstanding efforts by police to preempt and disrupt the activities of social movements and targeted communities. Discussing predictive policing in terms of its preemptive aims and harms captures the harmful operationalization of predictive logics.

Scholars also emphasize that, due to the racialized, discriminatory aspects of preemptive violence in the context of state action, it is in fact rather *predictable* who will be preemptively policed (Minocher and Randall, 2020). Therefore, Minocher and Randall propose calling predictive policing 'predictable policing' – pointing to the fact that, for all the high-tech data driven analytics apparently necessary to designate particular people as risks, the result continues historically well-documented discrimination and oppression. Another example of the definitional confusion surrounding anticipatory logics concerns the distinction between prevention and preemption in the context of risk-based governance of hazards, and the military operations of states. Andrejevic (2020) and Massumi (2015) both follow a line of critical security scholars such as Amoore (2013) de Goede and co-authors (2014) and Aradau, together with Van Munster (2008; 2012) to draw an epistemological and ontological line of separation between these two anticipatory logics. Prevention, these scholars argue in interrelated ways, is based on traditional, statistically constructed, and actuarial notions of calculable risk, while preemption (especially in the context of policing and war) is tied to the speculative and 'possibilistic' (c.f. Amoore, 2013) exploitation of the unknown towards particular political ends. The definitional confusions, slippages, and highly contextual ways in which different future-oriented modes of being and doing are described in the examples above are what lead me in this thesis to take up anticipation as an umbrella concept through which to make sense of practices and logics related to acting on probable futures (c.f. Anderson, 2007; 2010). In the context of my study of surveillance resistance, the concept of anticipation refers to the future-oriented dimension of action taken in avoidance of probable threats and harms. Following this definition, anticipation provides a frame that can encompass the complex, entwining forms of future-oriented reasoning and action that come into play through surveillance resistant practices.

Infrastructure and practice: a relational approach

Until now, I have mostly discussed resistance in the context of practices and logics. However, another important unit of analysis in my thesis is infrastructure. More specifically, I look at how the productive, anticipatory dimensions of resistance practices contribute to processes of security *infrastructuring,* as I explore in depth in Chapter 7. My thinking about the relationship between practice and infrastructure builds on the 'relational' approach to understanding practice and infrastructure developed by Susan Leigh Star and her co-authors (Star and Griesemer 1989; Star and Ruhleder, 1996; Star 1999; Bowker and Star, 1999). A relational approach to infrastructure casts practices as shifting entities that travel and give shape to different social worlds and their infrastructures. This approach understands practices and infrastructures as fluid entities that undergo shifts and changes over time and in response to the contestations of the different communities of practice that engage with it.

Especially at the start of my thesis, I found Star and Griesemer's work on boundary object theory (1989) generative for thinking through the coordination and contention by which 'transnational civil society' configures resistant practices and infrastructures. The 'boundary object' – a practice negotiated at the boundary and overlap of multiple communities – provided clues to me for how to trace the mobility of anticipatory data practices. I observed that anticipatory data practices were common to several different communities of practice involved in security that otherwise held conflicting values and goals. As I advanced through the thesis, I moved away from an explicit analysis of practices as boundary objects. However, Star and her co-authors' notion of an 'institutional ecology' – which she concurrently developed with the boundary object (1989) and Star's 'tricks' for reading infrastructure (1999) – helped to ground my research trajectory.

As a brief introduction to Star's thinking, Star developed the concept of the boundary object through a historical case study of Berkley's Museum of Vertebrate Zoology. Through archival research, she constructed an 'institutional ecology' of amateur and institutional participants whose engagement with the museum lead to the establishment of zoology as a formalized field. Her concept of institutional ecology grew out of her feminist critique of actor network theory in the late1980s. Star and Griesemer argued that Actor Network Theory focused too much on the perspectives of experts. In contrast, they argued that 'the viewpoint of the amateur is not inherently better or worse than that of the professionals' (1989. Star and Griesemer argued that an ecological approach was superior to a network-oriented one because it did not require assigning an 'epistemological primacy for any one viewpoint' (389). Constructing an institutional ecology allowed her to highlight the important contributions of amateurs to the formation of a new scientific field. As I will discuss more in my research design, I use the institutional ecology approach to trace the interrelations between NGOs, grassroots groups, and commercial and state actors as they converge around technological assemblages.

Star's article titled 'the ethnography of infrastructure' (1999) provided a set of 'tricks' for 'reading' infrastructure (384), which further informed my research approach. The first one she outlined was **'identifying master narratives and others'.** Star defines the master narrative as 'a single voice that does not problematize diversity... and which 'speaks unconsciously from the presumed center of things' (384). The master narrative comes into play in a number of places in my thesis where I challenge hegemonic conceptualizations of risk, anticipatory logics, and cybersecurity. For example, in Chapter 5 my co-author Stefania Milan and I examine the ambivalence of the focus by security specialists on the notion of 'awareness' as a panacea for surveillance and data-related harms. In Chapters 4 and 7 I examine how surveillance risks and threats are framed according to security specialists from wealthy 'global north' countries. In Chapter 7 I examine the standardization politics and

hegemonic anticipatory logics bound up in the infrastructuring of digital rapid response and security threat intelligence.

The second 'trick' laid out by Star involves **'surfacing invisible work,'** or 'articulation work' (385). One form of articulation work that appears throughout my thesis is anticipation (c.f. Clarke, 2016), which I discuss as an affective and temporal orientation that helps articulate priorities for security and safety and gives shape to security infrastructures. In Chapters 4 and 7, I discuss anticipation as a form of articulation work that ties together the 'dance of surveillance' and resistance (c.f. Marx, 2009). A third 'trick' that heavily informs my thesis is the **'paradoxes of infrastructure'** (386), which Star refers to the 'barriers and obstacles to users of technical 'tools' and features'. My thesis starts from the assumption that security presents barriers and obstacles, from the dangers and uncertainties people must navigate to the brittle and difficult to use nature of tools. Whereas in the past I focused my studies on the difficult nature of 'digital security tool' use and the challenges of security practice integration (Kazansky, 2015; 2016), my thesis has a different emphasis. Rather than focusing on these tools, I examine how people rely on anticipatory modes to determine which tools are appropriate in light of these barriers and obstacles.

Conclusion

This chapter has discussed how I engage with several different literatures related to technological practices, resistance, activism, and infrastructures. I have argued that the study of surveillance resistance has illuminated many important and only lightly trodden paths that are worthy of further exploration. Also, I have explained how I articulate my concerns with anticipation in the context of daily security practices and security

infrastructures within civil society. The next chapter of the thesis explains my research design, discussing how the empirical trajectory of my research came together to enable me to explore anticipation through a multi-sited ethnographic study of practice.