What harms may come?

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

Kazansky, B.

Publication date
2021

Chapter 3. Research Design

Introduction

This thesis focuses on the coordination and contestations between global non-governmental organizations, grassroots collectives, local groups, and technical specialists focused on bolstering digital security, safety, privacy, and autonomy amidst the threats of digital surveillance and datafication. It draws on qualitative data collected through ethnographic participant observation at 12 conferences and events, 50 semi-structured interviews, and a close reading of 120 'grey literature' documents encoding and explicating civil society practices related to security and surveillance resistance. Fieldwork and data collection took place between 2016–2019. The methods, research sites, and thematic analyses of the thesis are informed by my goal of identifying and tracing how anticipatory logics circulate throughout the practices and infrastructures of civil society's ecology of actors working to counter the threats and harms of surveillance and datafication. This chapter will discuss in more detail how research sites and methods were chosen and bounded; how data was analysed; and the epistemological and ethical considerations that have framed my research approach.

Research Approach: towards a critically engaged sensibility

The epistemological and methodological basis for my thesis emerges from my background in action-based research and practice in relation to technology, human rights, and social justice (Kazansky, 2015; 2016). In particular, my time working as a researcher and educator on matters of digital security and privacy with non-governmental organizations in the US, Europe and Asia was formative to the development of my research

sensibility, which seeks a critically engaged approach to the study of technology and society. An important point of departure of this PhD project was the recognition that as a researcher, I am not a detached observer of an outside world (c.f. Law, 2004). As such, how I formulate my research questions is necessarily tied to broader commitments in relation to human rights and social justice. As I have negotiated my position as a practitioner and scholar, I found the 'research justice' (Jolivette, 2015) framework important to articulating my research approach. This framework describes how to operationalize a set of commitments for communities who research and are researched. These commitments entail empowering research participants to determine the conditions of their participation, and honouring their contributions as valid forms of knowledge. The research justice ethos finds a corollary in feminist technoscience, which counters attitudes in academe that insist on the notion of objectivity premised on a 'view from above, from nowhere' (Haraway, 1988: 589). Haraway's injunction to recognize 'partial' and 'situated knowledges' as a valid and vital contribution to knowledge production necessitates alignment with issues of epistemic justice. Similarly, proponents of research justice argue that it would be irresponsible to conduct research without having commitments in place that guide the researcher on matters of ethics, epistemic justice, and the overall goals of the research. These considerations are central to my ethico-political approach towards research sites and research participants.

At first glance, being both a 'critical' and 'engaged' researcher might appear contradictory, eliciting questions about how much distance is appropriate for a researcher to take from their subject matter or communities of study. At the beginning of my thesis, this distance underwent negotiation as I was pushed to develop a critical distance to my prior work as a practitioner to better articulate my identity as an academic researcher. Attaining an appropriate critical distance towards 'the field' did not involve a radical of a departure from my prior work. Rather, my thesis germinated from a desire to study my own field of practice

critically. Furthermore, my previous practitioner research was premised on a reflexive approach to practice that relied on critically interrogating the tropes of my own work and institutional context (see: Kazansky, 2015; 2016). Yet, just as critical distance was deemed necessary, so was continued proximity. To make sure that my research remained engaged with the troubles of my field of study, I endeavoured to develop research questions that were salient not just for the academic communities involved in studies of technology, social justice, and human rights, but also for others engaged in the work that I study.

As such, I formulated research questions to address concerns within civil society about the harms of surveillance and datafication. Cognizant of my responsibility to support and respect the ambivalent and complex realities of civil society work, my approach was to develop a critical lens that drew upon critical questions and contestations present in the field itself. As I already mentioned in the introduction to the thesis, some of the contested matters that engrossed me during my practitioner years involved how 'we' as practitioners, working to raise awareness of surveillance concerns and every-day vulnerabilities, talk and think about threats and risks and conceptualize uncertainty. In the workshops and discussions I attended, digital security trainers and advocates often tried to suss out the drawbacks/positives of particular frameworks and methodologies for 'managing' and mitigating surveillance concerns. The arguments we had were central to the development of 'best practices' in our communities of practice. Within academe, our critical discussions could be understood as a form of proximal critique that stayed close to practice. I found this to be a crucial base from which to construct my research questions.

To further articulate a 'critically engaged' approach to research for my research project, I collaborated with my colleagues within the DATACTIVE team. In a working paper on the ethics and positionality of the collective DATACTIVE project, Stefania Milan and I outlined what such an approach would mean at the project level. This description broadly applies to my individual project as well:

> DATACTIVE adopts an ‘engaged’ approach to research (Milan, 2010, 2014), by virtue of which we interrogate the impact that our empirical inquiry might have on people and communities, and strive to contribute to the goals and causes of the communities we address (see also C. Milan & Milan, 2016). Put it differently, DATACTIVE seeks to do research ‘with' instead of 'about', thus entering into a continuous dialogue with the fields of action and interaction being observed (cf. Charlotte Ryan, Salas-Wright, Anastario, & Camara, 2010). This entails, for example, focusing as much as possible on research questions that are relevant to both the researchers and to the field that is being studied; honoring and attributing the sources of ‘situated knowledges’ (Haraway, 1988); seeking appropriate opportunities for co-inquiry, exchange, and collaboration; and taking great care towards how we collect, handle and present data about identities, projects, networks, and group dynamics. Data security and privacy related practices are thus made a central element of our overall approach. But, most importantly, we recursively ask ourselves what are the epistemological and ontological consequences of 'doing research with’, and what potential risks these might harbor. Among the latent risks are (a) doing potential harm to those we do research with, and (b) losing space for critique with respect to our research subjects.[2]

Regarding issues of ‘research ethics,’ as part of the critically engaged approach, it would be necessary to conduct research through epistemically just methods attuned to the safety and goals of research subjects and relevant communities. I will outline these in more detail later in the chapter. Next, I structured my research to facilitate inductive theory development. As I will outline in more detail later in this chapter, my

2 Our ethics working paper is available to read here: https://data-activism.net/wordpress/wp-content/uploads/2021/07/DATACTIVE_ethicsWP-4.pdf

fieldwork and analysis were conducted iteratively, with each cycle building on the last. Findings were then shared back with respondents, discussed, and occasionally re-articulated to better reflect the perspectives shared with me. Considering my own history and positionality, the inductive approach I took allowed me to acknowledge my prior participation in the field, reflecting on my own expertise and intuitions as a practitioner in my field of study. Simultaneously, it also enabled me to take steps to de-familiarise myself from it by making a conscious effort to explore unexpected field sites and practices in order to allow my analysis to emerge from the material. Finally, as part of my feminist commitment to look beyond the 'master narrative' of technological progress (c.f. Star, 1999), I tried to 'stay with the trouble' (Haraway, 2016) of persistent problems (i.e. resource constraints, historical patterns of dispossession, infrastructural breakdown, and reconfiguration) in a quickly changing field. It was equally important to also trace shifts in problem definitions over time, such as from privacy and digital security to data politics and AI. These shifts in attention economy and problem definitions remain central themes in the thesis.

Constructing the research site

My goal was to study practices as they circulate across sectors, communities of practice, and particular contexts of enactment. Hence, it was clear in the formative phase of the thesis that my research would cut across numerous physical and virtual sites. This elicited questions about how to construct and 'bound' a patchwork of diffuse yet connected research sites. Not only were the research sites diffuse, but my engagement in fieldwork itself had an episodic rhythm, largely organized around week-long annual conferences. I gained gained to periodic meetings and workshops, the organization of which remained beyond my control. The methodological work of ethnographer Jenna Burrell (2009)

was useful to think through how to delimit my research sites. She writes, in relation to her research on Internet infrastructure, as inspired by Marcus (1998a, b), that:

> 'contemporary ethnography is often a study of parts rather than wholes. Researchers cycle in and out of the field, skip certain areas entirely, and may rely on the recollections of participants in interviews to map out the space' (186).

Though my episodic fieldwork meant that I did not engage in months-long stretches of continuous, immersive fieldwork, that did not prove detrimental to my research goals. By the beginning of this academic research project, I had already spent seven years deeply immersed as both a participant and a researcher in the study of the field at hand. The above combination of factors also brought me to explore methodologies for ethnographic research that go beyond traditionally bounded research sites. The question, as framed by Burrell, is: how to construct a research site that 'incorporates physical, virtual, and imagined spaces' (181) and which is not traditionally bounded? Burrell traces a trans-disciplinary shift in methodological approaches to ethnography to account for the contemporary 'movement of objects, of individuals, of ideas' (183). She draws on Marcus' notion of multi-sited ethnography (1998) to conceptualize how research projects can be coherent 'without being spatially bounded (183). Marcus, in turn, writes of 'multi-sited ethnography' that:

> moves out from the single sites and local situations of conventional ethnographic research designs to examine the circulation of cultural meanings, objects, and identities in diffuse time-space. This mode defines for itself an object of study that cannot be accounted for ethnographically by remaining focused on a single site of intensive investigation (Marcus, 1998: 79–80).

How to construct such a multi-sited ethnographic study for the purposes of my research? The idea for a multi-sited ethnographic study of technological infrastructure and practice became concrete through my engagement with Susan Leigh Star's work. Star teases out the temporally and spatially diffuse nature of information infrastructures and the coordination that goes into its development. Taking inspiration from Star's work studying how practices change through the participation of different social groups (c.f. Star and Grisemer, 1989), I planned to construct and study a loose 'institutional ecology' of the organizations, collectives, and technological infrastructure bound up in civil society's promotion of digital security, digital rights, and resistance to algorithmic harms. The notion of an institutional ecology is drawn from Star and Griesemer's study of standardizing practices around the museum of zoology (1989), as well as Star and Ruhleder's study of worm research software (1996), as I mentioned in the last chapter.

The institutional ecologies I constructed emerged from several activities. In the first months of my PhD, I made an initial mapping of relations between several dozen NGOs and grassroots groups working across transnational configurations to build and maintain technical infrastructures meant to counter the harms of surveillance and mitigate digital threats, basing it on desk research and my own background in the field[3]. I grouped these different actors and traced their interrelations by their issue focus, size, and degree of institutionalisation; disparities in resources; geographic scope of work; and political commitments, epistemologies, and expressed values. My goal was not to simply draw a line of connection between different actors, but to trace dependencies, contestations, and collaborations between the different NGOs, grassroots groups and technological projects. As part of my focus on locating the 'located accountabilities' of technological production (riffing on Suchman, 2002),

3 I later engaged in a similar mapping exercise of 'data activist' actors together with the DATACTIVE group as part of our initial research activities together.

I attuned myself to tensions emerging between tech-centric actors such as security specialists and infrastructure service providers, with the affected communities imagined and positioned as the 'users' of their services and expertise. I drew upon this initial institutional ecology to guide interview and field site selection for the project. Over the course of my fieldwork, this single institutional ecology turned into many, grouped according to the particular themes and events of study foregrounded in the five chapters that form the core of the thesis.

Data collection strategies

Interviews, participant observation, and document analysis were equally important to my research. Interviews allowed me to identify emerging priorities in the field; discuss different epistemologies around risks and threats; and explore why practices are configured and enacted in particular ways. Interviews also opened opportunities to visit otherwise closed field sites, such as digital security trainings and confidential meetings. Participant observation allowed me to understand the embodied and intersubjective dimensions of practice; to see how practices are enacted in a certain place and time; and to observe the collective process of sense-making and threat construction as undertaken through different forms of risk assessment, threat modelling, and other practices discussed in interviews. Finally, document analysis allowed me to understand how practices are formalized and encoded over time, and to observe shifts in the priorities and problem definitions of civil society organizations and technical project teams.

My ethnographic fieldwork was conducted both laterally and longitudinally. First, I laterally studied the interactions taking place within and across 'institutional ecologies' emerging from the interrelations of transnationally coordinating civil society organizations, collectives, and

allied individuals involved in countering the harms of surveillance and digital vulnerabilities. Second, through the study of these relations, I engaged in the longitudinal selection and deepening of my study of discussions and enactments of sociotechnical practice taking place at the site of particular conferences, workshops, and events. This study united thick description and 'thin' description (c.f. Benjamin; 2019; Hoffman, 2020) of technological practice, as well as the values and politics imbricated therein. By thick description, I refer to description of practice as it is enacted, embodied, and discussed. By 'thin' description, I refer to my efforts to trace the relationships of practices, infrastructures, and people across different sites. This combined approach allowed me to explore the relationship between different sites of practice and moments of their enactment, as per my goal to engage in multi-sited ethnographic research.

Interviews and interviewees

I conducted a total of 50 semi-structured interviews between 2016–2019, with civil society actors from a total of 26 countries in different regions of the world, including the Middle East and North Africa Region, Southeast Asia, South Asia, Central Asia and the former Soviet region, Eastern Africa, South Africa, West Africa, North America, Central America, South America, Western Europe, Southern Europe, and Eastern Europe. These interviews did not actually take place in 26 countries, but at twelve international conferences and workshops taking place in Europe and Southeast Asia, and in some cases remotely. The fact that interviewees come from 26 countries is a result of the demographics of the gatherings where the fieldwork was done, which itself is representative of the transnational configuration of NGOs and grassroots groups (c.f. Price, 2003 engaged in various degrees of dialogue, collaboration and contestation on issues relating to digital rights, Internet freedom, digital security, and technologically related discrimination and injustice. The physical events where these interviews took place serve as international

meeting points for NGO representatives, community organizers, security experts and technologists to come together to coordinate their transnational and trans-regional work to mitigate and respond to the harms of digital surveillance and digital threats.

Interviewees were selected through purposeful sampling. They were chosen for their contributions to security and counter-surveillance practices as educators (digital security trainers and facilitators), technologists (infrastructure service providers, hackers, and software developers), and representatives/members of affected communities, as well as 'users' of software and infrastructure (self-described community organizers, human rights defenders, and people subject to oppressive surveillance measures and digital attacks). Interviewees came from varied backgrounds, affiliations, and orientations to their work. Some focused their work locally while others took a cosmopolitan and transnational approach. This broad selection of interviewees included people explicitly working on technology issues related to Internet freedom, digital rights, human rights, and social justice – as well as people engaged in this arena proximally – through a concern with how technologically related threats are affecting their human rights or social justice issues. These technology 'adjacent' issues included environmental justice, anti-racism, violence against women, transparency, accountability, anti-corruption, labour organizing, and various related intersections.

To provide more detail on my respondents, the first category of people interviewed consisted of constituent populations & infrastructure 'users'. This category referred to human rights defenders and activists participating in digital security trainings; people requesting services from NGOs, security specialists and technical service providers, and members of software user groups relevant to the software projects of study. These included people serving as representatives from labour unions, women's rights activists, LGTBQIA+ activists; Indigenous land rights defenders, and community activists fighting against predictive policing regimes in

the United States. The second category of interviewees consisted of educators, which included facilitators of workshops and digital security trainers. These educators work with human rights defenders and movements to raise awareness of different kinds of digital threats, increase technological literacy and promote countermeasures such as VPNs and encrypted messaging apps. The third and final category consisted of technologists. Within the technologist category, I placed commercial and state actors providing services to and collaborating on civil society infrastructures. This category included people identifying as hackers; system administrators; developers of privacy-enhancing technologies and digital security tools; and other people primarily concerned with the functioning of technological infrastructures.

Among interviewees, there was a significant degree of overlap between people identifying as technologists, educators, and human rights defenders and community organizers. This overlap speaks to the leakiness of my categories and the career paths that have brought people to particular roles and areas of work within 'civil society'. On the other hand, as already mentioned in the introduction, some people explicitly did *not* identify as civil society actors. Instead, they chose to describe themselves as community organizers, among other roles. In the absence of consensus around a better word to describe the broader field dealing with issues of human rights and social justice as it pertains to technological harm, I have tried to stick closely to the self-descriptions and identifiers used by the different groups and individuals I have interviewed. In the many instances where interviewees framed their work as part of 'civil society', I have used that term. In cases where people expressed an issue with this term or defined their work through another one, I have foregrounded their preferred term. This has been a challenge as there is also a need for some uniformity in the text, first and foremost for its readability. I have tried to balance these two needs in the most legible way possible.

Structure of interviews

The interviews were semi-structured, and geared towards the exploration of values, experiences, and practices. A list of semi-structured questions was prepared in advance, which were changed or supplemented depending on the course of the conversation that developed during the interview. These questions drew from two sources: a common DATACTIVE questionnaire, and questions tailored to my project, which focused on surfacing issues around threats of concern to the interviewee and the communities they support[4]. I conducted background research ahead of the interview to collect data on the interviewee's projects and their organizational context, which further informed the question preparation. Interviews lasted between 45 minutes and 1.5 hours. They were arranged over encrypted email (where possible and advisable) or after meeting interviewees at conferences, meetings, and workshops. In my interviews I worked to achieve 'data saturation' (Faulkner and Trotter, 2017) around prevalent points of discussion, threats of concern, emerging technical projects, and advocacy initiatives of interest. Topics covered in each interview included: how did the person first get involved in their field of work; what do they believe to be the most important and pressing concerns around technology, surveillance, and digital security; what threats do they focus on addressing with their constituent communities; and how do they perceive the field to have changed over the years they have worked in it. Interviewees were asked to reflect on and describe the tactics and strategies they use to identify and counter 'digital' threats. Discussions spontaneously turned to issues of specific technical tools and projects; the variety of different issues they believe to be pressing and important; and the abstract concepts and practical details of the work.

4 Please see the Methodological Annex at the end of the thesis to view interview questionnaires prepared for two different interviews, as well as some further information about interviewees.

Interviews are referred to throughout the text following a uniform scheme, from Interview #1 to Interview #47. Some of these interviews were conducted with multiple people, and the total number of interviewees added up to 50. This interview scheme is anonymized and intentionally contains no metadata relating to the year they were conducted or their concrete location. However, the scheme corresponds to a separate set of interview codes, which does contain this metadata. Because the interviews I conducted were part of a larger corpus of 250 interviews conducted by the DATACTIVE project team, my interview metadata has been stored in encrypted form by the Principle Investigator of the DATACTIVE project in accordance with the European Research Council.

Participant Observation

Participant observation was conducted at a dozen conferences, workshops, and meetups that took place across Europe and in Southeast Asia. Participant observation allowed me to gain a deep understanding of how practices are enacted in a particular place and time. It also allowed me to learn about the most important problems, priorities, and controversies of the field. Finally, the interaction afforded by participant observation also facilitated the selection of additional interviewees. During the course of participant observation, I took notes. Immediately afterwards, I made memos about striking moments of discussion and other highlights from my participant observation. My notes were recorded in a paper notebook or on my laptop. All names of people and organizations were immediately anonymized. Later on, the notes were collated and analysed alongside interviews. There were several cases where, through pre-agreement, I wrote confidential reports using these notes and shared them back (in anonymized form) with the organizers of events to provide them with useful information for their digital security capacity building efforts. During my field work I made a total of four such reports, each between 3–

5 pages, and discussed them with the hosts of the event convenors. In the section below I describe the different settings where I conducted participant observation.

International Internet freedom and digital rights conferences

As part of my participant observation, I attended three years (2016–2019) of a digital rights and Internet freedom conference taking place in Europe, which always lasted seven days. This event brought together approximately 1000 participants from every region of the world, providing an important meeting point for digital rights, privacy, digital security, and Internet freedom NGO workers, security specialists, movement representatives, and technologists coordinating transnationally and trans-regionally with different global regions. Over the course of three years, the event organizers increased funding for participants to be able to join in person from 'global south' regions, thus the diversity of participants markedly increased over the three years I attended. At this conference, participants showcased new projects about technical circumvention tools and digital security mitigation strategies; discussed best practices for capacity building, funding, and advocacy; and set priorities and agendas for future collaborations. Each conference contained a mix of large information sessions and smaller workshops, covering topics such as emerging policy concerns, educational pedagogy for digital security trainings, reports on digital attack patterns and mitigations, and discussions about diversity, racism, misogyny and abuse within the digital rights and Internet freedom community. At big presentations and smaller workshops, I would introduce myself as a researcher to presenters or participants who made salient points, and I would ask if I could conduct a follow-up interview with them. Many times, I also contacted presenters or attendees ahead of time to schedule

interviews, however being able to chat in person was often important to establishing trust and breaking through the noise of the busy conference. During these interviews, several interlocutors also staged software demos or let me play with the software projects they were involved in.

International Hacker camps and conferences

I attended three years of large hacker conferences in Europe (2016–2019), each lasting five to seven days and with attendances of approximately two to three thousand people. Just like the Internet freedom and digital rights conferences I attended, hacker camps also served as international meeting points for people from disparate geographies but of converging interests. It should be noted that a greater majority of participants came from Europe and the US rather than the majority world due to affordability and other issues of class and diversity. These events attracted a greater number of security specialists working in commercial, government, and autonomous hacker space contexts (rather than specialists working with NGOs and movements), self-identified 'hackers' of different stripes, and a smaller niche of digital rights and Internet freedom groups and projects. This category of event was distinguished by a heavier focus on the innards of technology and was concerned with hands-on activities to build, tinker with, and take apart technical infrastructures. In addition to large lectures covering themes around security and emerging threats, there were also many meetups for particular technology 'user' groups and informal 'villages' of people sharing particular niche interests. Prior to attending hacker camps, I would scan the programme to identify emerging themes and then attend as many sessions as possible to get a birds-eye view of them. As with the Internet freedom and digital rights conferences, I would either email presenters and participants ahead of time or introduce myself as a researcher at different sessions and ask if I could conduct a follow-up interview.

Closed digital security trainings and private meetings

In addition to the above events, I attended 12 smaller, closed workshops organised to develop specialised tactics and strategies of defence from digital attacks and surveillance related issues. Some workshops observed focused on the tactical application of tools to counter privacy, security, and surveillance concerns, while others broached conceptual issues related to digital and 'data literacy', exploring 'data politics' and issues around diversity and social justice as it relates to the work of the affected communities involved. I gained access to these workshops only following a period of building trust with the organizers. Within these 12 events, I attended two longer digital security trainings between 3–5 days long, which provided me an important opportunity to observe the development and enactment of practice and strategy. The first of these trainings focused on digital security for human rights defenders at risk, covering topics of 'data politics', censorship circumvention, secure data storage, and secure communication. This training brought together participants from all over the world, many of whom had left urgent circumstances in their work to counter violence against women, environmental destruction, and corruption. The second training focused on the inauguration of a secure communication platform for a small network of journalists in Southeast Asia. Unlike the general curriculum of the first training, this group was there to learn a particular 'toolchain' of security measures to operationalize their goal of communicating safely with whistleblowers and media outlets.

Participation at these private workshops and events followed only after an assessment, conducted together with organizers and participants, to ensure that the presence of a researcher would not be disruptive or compromise the safety of anyone involved. Further, I provided an analysis of my observations back to the organizers directly following my attendance to

gain a sense of research topics that should be avoided for safety reasons. These reports also served as an action-oriented outcome, allowing me to immediately provide information that might be directly useful to the organizer and attendees. These reports were 2–3 pages long and surfaced the concerns and expectations expressed by attendees; main topics of discussion; and main concerns around security and safety. The format of these reports was influenced by my prior work in the field, through which I came to know what kinds of information would be salient and useful to people conducting trainings or engaging in other security related issues.

Document analysis

In-person observation and interviews were supplemented with close readings of user software 'walk-throughs', software usage guidebooks, tactical playbooks, security self-defence manuals, security marketing materials, educational guides for understanding security issues, pedagogical guides for how to conduct risk assessment and threat modelling, and NGO reports about security threats. The materials I looked at were published from 2007–2020 by different civil society organisations, technical service providers, and security specialist bodies involved in surveillance self-defence, digital security, privacy, and safety. I noted that 2007 was the earliest year these issues were predominantly recorded and documented in online materials, guides, and playbooks produced by the Internet freedom, digital security, and related organizations whose outputs I studied. These documents were produced by organizations including the Electronic Frontier Foundation, Tactical Technology Collective, the Tor project, Protection International, Front Line Defenders, Access Now, Internews, the Engine Room, the Association for Progressive

Communications, Derechos Digitales, CyberSeguras, Coding Rights, FIRST, QubesOS, Dowse, and a number of others[5].

The documents I studied should be understood as important texts for elucidating the discourse and practices of civil society, for it is in these texts that methodologies and epistemes around surveillance, security, privacy, and related subjects that have been fleshed out through debate and practice are encoded, distilled, and promoted. This was revealed by the fact that interviewees often expressed strong opinions about the merit of particular guides related to security mitigations and everyday practices, offering impassioned critiques on their particular inadequacies, relative relevance, and respective completeness. I analysed a total of 120 different documents, which I selected according through several criteria: a. they were referred to in interviews; b. they were discussed at conferences were participation observation took place; c. they were referenced in other guides put together by civil society organizations, or d. they were promoted, or discussed on social media (Twitter) by digital rights, digital security, and human rights practitioners. My goal in the close reading of these manuals was to analyse the values, imaginaries, and logics implicit to methodologies for assessing and mitigating threats. I was interested in understanding how the manuals frame notions of risk, threat, security, and privacy. How did they differ or build off of one another? What kinds of inconsistencies did they expose regarding tactics and strategies and mitigations featured? How were threats and risks constructed and presented to their respective audiences?

5 The documents which are analysed throughout the text of the thesis have been incorporated into my References section. Some of the documents analysed are confidential, and therefore not quoted, nor included in my references.

Research trajectory

This thesis is organized into five thematic analyses related to the anticipatory dimensions of resistance and response to the harms of surveillance. In the section below, I explain how these five thematic explorations were constructed through iterative analysis.

1. Desk research

My thesis research began on the heels of a recently completed research project looking at the challenges of privacy and digital security practices amongst human rights defenders (Kazansky, 2015; 2016). Conducted as an action-oriented research project within a practitioner organization, the project conducted 60 interviews with human rights defenders and several extensive case studies drawing on fieldwork that involved participatory workshops and meetings. This project played a concrete role in shaping my positionality as a critically engaged researcher, providing me with a ground-level understanding of the field. While this was an asset, it also required me to consciously de-familiarise myself from the field in which I had been a participant. My de-familiarisation was aided by a period of desk research undertaken at the start of the project, during which time I homed in on several critical concerns that I would later explore through this new phase of research with the DATACTIVE project. Desk research involved the textual analysis of documents published by civil society organizations, including policy briefs and security and technology guides. This allowed me to assemble formative questions, identify potential interviewees, and surface potential themes to be explored further through my fieldwork.

2. Exploratory interviews and participant observation conducted at conferences with civil society actors from different regions of the world

In the first phase of my fieldwork (late 2016–early 2017), I attended two 3 to 4-day meetings bringing together trainers and human rights defenders from around the world to discuss how to address digital security issues, as well as two large 4–5 day conferences covering a number of different topics. One of these conferences was organized to bring together an international 'hacker community' and the other was organized to bring together transnationally coordinated Internet freedom and digital rights communities. In preparation for these events, I scanned conference programs looking for recurring topical themes in the description of panel sessions, interactive workshops, and technical demonstrations. Looking back on the programmes of events I attended from 2016–2019, the topical focus of workshops, talks and demonstrations shifted slightly from year to year. For example, in 2017, while attending a large digital rights conference, I noted that the programme included several different workshops aiming to discuss the merits of different kinds of threat modelling and risk assessment methodologies. When I went back in 2019, I noted that the same conference had far fewer workshops on how to model threats and assess risk, and many more about imagining 'hopeful' futures. There is no way for me to know now if this was a result of fewer people submitting workshops on threat modelling and risk assessment, or if the organizers of the conference had chosen a particular direction for the conference. Likely it was a mix of both. My initial theory was that as risk assessment and threat modelling methodologies have become more formalized and imbricated within civil repertoires, a desire arose to focus not just on the avoidance of undesirable futures, but on practices centring hopeful speculation and feminist fabulation (c.f. Haraway, 2016). The turn toward fabulation coincided and intertwined with a growing interest amongst civil society actors concerned with surveillance with practices of

refusal and abolitionist strategies. I explore the topic of abolitionist community organizing and how it was discussed at this digital rights conference in Chapter 8 of this thesis.

Coming back to the start of my fieldwork, based on the thematic patterns identified in event programmes published in 2016 and 2017, I identified a variety of talks to attend and workshops to participate in. At these talks and workshops, I would take notes on the discussion (immediately anonymizing who said what) and identify individuals and groups for potential interviews. Notably, I sometimes arrived at an event with a predetermined idea of who would be interesting to speak to on account of their specialist focus on a particular subject, or experience and positioning within civil society. These predetermined ideas resulted from the prior desk research I had done, and the institutional ecologies I had constructed.

I organized interviews in two ways. As a first option, I would introduce myself to potential interviewees immediately after they had presented on their work, attempting to conduct the interview later at the event. As a second option, if this was not possible, I would send an email afterwards to propose a remote interview through an agreed upon VOIP platform meeting GDPR standards. In this exploratory phase of research, I conducted a total of 12 interviews, aiming to achieve adequate diversity with regards to area of expertise and concern, gender, and geographic representation. These 12 interviewees included technologists (such as software developers and infrastructure service providers), security experts (such as trainers/educators), and human rights defenders and community organizers from different regions of the world.

3. First stage of thematic analysis

With 12 initial ‘exploratory’ interviews completed and field notes gathered from several events, I conducted an initial analysis of my data, focused on surfacing recurring and salient themes. I followed a ‘reflexive

thematic analysis' approach (Braun and Clarke, 2019) through which 'patterns are identified through a rigorous process of data familiarisation, data coding, and theme development and revision' (Braun and Clarke, n.d.). In terms of the identification of patterns, I focused on identifying how individuals and groups anticipate, respond to, and prevent future digital threats and surveillance. I also homed in on the interviewees' reflections regarding how civil society and technology work has changed over the years that they had engaged on issuers related to security, privacy, human rights, and social justice. Equally, I sought to capture emerging priorities about surveillance concerns, mitigations, and civil society practices. In this section I provide a brief overview of the themes that emerged during this period of analysis. Through my analysis, I identified an overarching tension between the many persistent problems faced by civil society actors (such as small NGOs and grassroots groups not being able to afford technology support or licensed software) and anxiety over the threats and harms of emergent high technologies and systems (such as the spread of 'smart' biometric surveillance systems worldwide).

The twelve respondents interviewed in this exploratory stage of research expressed an urgent need to formalize and professionalize responses to security and surveillance incidents through new collective mechanisms such as threat intelligence platforms to track security threats and attacks, repositories of information relating to how attacks are conducted on different communities, and rapid-response help desks able to offer emergency support to those subject to attacks. This became the main theme of Chapter 7. Respondents also showed excitement over nascent technical projects such as hardened computing systems which prioritise compartmentalisation and resilience to different forms of digital attacks (explored in Chapter 5). Further, several interviewees discussed the need for civil society to articulate its stance towards artificial intelligence systems and discrimination in relation to issues of digital security privacy. At the same time, interviewees expressed ambivalence towards

technological ‘hype’ in this area, worrying that spreading too much fear and concern about an issue still remote from the daily work of many could backfire (also explored in Chapter 4 and Chapter 5). On the other hand, all interviewees acknowledged a need to rethink security, safety, and privacy strategies, considering widespread corporate data exploitation. This became an important main theme of Chapters 4, 5, and 8, as part of my exploration of shifting technical priorities and problem definitions.

Next, many respondents argued for a need to reframe discourse and practice around risk, security, and safety to account for the concerns over diversity, colonialism, racism, misogyny as they arise within civil society, highlighting that experts from the ‘north’ still presided as gatekeepers and held outsize authority in shaping the direction of the field. The Inequity of resources and funding between civil society in wealthier North American and Western European countries and those in the majority world was a continued source of strife. These issues were essential to my analyses across all five core thesis chapters.

Finally, future-oriented, anticipatory modes of thinking and doing (such as prediction, prevention, preemption, and speculation) were a central undercurrent of every discussion I engaged in or observed around threats and harms, shaping the language used to discuss past, current, and future priorities and uncertainties. As a result, the future-oriented dimensions of surveillance resistance became the central lens of my analysis, through which I explored the other themes I already highlighted above. Respondents often argued for the need to more effectively gauge and communicate risk, speaking to the need for more attention to threat modelling to better contextualize concerns about data, surveillance, and related digital threats. The title of Chapter 4 refers to a common phrase I came across in both my practitioner work as well as when I spoke with respondents and asked them which technological threats they found most concerning to their work and to the communities they work with, namely that it ‘depends on your threat model’. Finally, in my interviews, many people drew an explicit line around needing to act ‘proactively’ rather

than ‘reactively’ to anticipated future threats. What exactly needed to be addressed more proactively varied widely, but the call for proactivity was widespread, with respondents calling for more trainings on preparedness for different threats, the development of new technical infrastructures, and the urgent abolition of unjust technological systems. This widely expressed imperative to act proactively became the central theme of Chapter 8.

During my fieldwork, I compiled and analysed a corpus of field notes in addition to a corpus of primary ‘grey literature’ texts produced by civil society, which I analysed alongside interviews. The coding of interviews, fieldwork and analysed documents was done through a ‘general inductive approach’ (Thomas, 2003), which allowed themes to be articulated through the analytic process. As my analysis work progressed, I took a more deductive approach to coding, regrouping coded material thematically and renaming themes to better reflect the patterns I identified across the corpus of data. For coding, I repurposed a software program called Scrivener. Scrivener is a locally installed commercial software program built to facilitate easy organization of writing material. I chose this software for coding because it allowed me to easily annotate my data throughout the process of pattern and theme identification and analysis. My coding took place in three stages. The first stage constituted ‘open’ (in vivo) coding, in which I coded names of projects, people and organization names; types of practices and work; expressed priorities and motivations; and recurring concepts around surveillance threats and surveillance threat response. The second stage consisted of axial coding, through which I began to identify and name recurring themes. In the third stage, I began to sort and group codes under broader thematic headings, and to rename these headings to best represent the patterns identified in my data corpus. This third stage of coding provided me with ideas for how to structure the five core chapters of this thesis. As I will explain further in the next

section, the process of analysis did not end there: As I later began to outline each chapter, I engaged in further thematic analysis.[6]

4. Further interviews with groups and individuals for each thematic exploration

Following the initial thematic analysis of interviews, field notes, and documents, I planned further fieldwork and interviews in order to explore emerging themes in more depth. For each thematic exploration in this thesis, I sought to trace the involvement of all of the kinds of people involved in development of practices and infrastructures to counter surveillance and digital threats, including individuals and groups affected by particular forms of surveillance, developers, software maintainers, and community outreach specialists. This was in line with my approach to 'locating accountabilities' (c.f. Suchman, 2002) in technological development and practice. To give a concrete example of how this played out, I briefly give an overview of the data collection that went into a couple of the core thesis chapters. Chapter 7 sketches out the institutional ecology implicated in the development and coordination of civil society's digital 'rapid response' mechanisms. The chapter describes what was defined by many interviewees as a crucial and growing field of practice focused on quickly intervening in 'digital emergencies'. The struggle to rapidly coordinate to counter digital threats emerged as a recurring theme in my inductive analysis of the initial interviews and field observation, which led to the snowball selection of further interviewees active in digital security rapid response. Interviewees included staff of established international NGOs, digital security specialists working with local

6 In addition to my individual coding process, I also engaged in a number of hours of coding following the official coding scheme of the DATACTIVE project, which was structured in a more deductive way. This coding was done on an autonomous, self-hosted coding infrastructure built by the DATACTIVE team and outside software developers.

grassroots groups, and cybersecurity technicians and service providers working with both civil society organizations, companies, and governments. The fieldwork and interviews allowed me to explore collaborations and contestations within an institutional ecology consisting of three kinds of digital security rapid response actors, identified in this chapter as global rapid response actors, local rapid response actors, and technical rapid response actors.

Chapter 5 deals with the study of 'algorithmic counter-imaginaries'. It explores how three small software projects try to intervene by offering other ways of computing and conceiving of datafication. My co-author and I discuss the QubesOS secure computing project, the Dowse project, and CV Dazzle. In exploring each of these three projects, I conducted desk research looking at software specifications and marketing materials. I also looked at online discourse among its users, particularly on Twitter and in online user forums. To explore the QubesOS project further, I attended several different events, including a workshop designed to help the open-source project developers surface concerns and priorities around the user experience of the project, as well as a meeting bringing together its diffuse and international user community. Adjacent to these events, I planned interviews with developers, users, and the imagined communities that the developers hoped to reach. This was a way to understand the imaginaries guiding the development of the software as well as the everyday frustrations and workarounds developed by its users. Another project featured in Chapter 5 is Dowse. For our study of Dowse, I attended an advertised meetup for IoT tinkerers, where Dowse was featured as an exciting new initiative to bring more control over the Internet of Things to 'end users'. Additionally, my co-author Stefania Milan involved the core developers of Dowse in a focus group discussion. Finally, I participated in a workshop about how to raise awareness to and counter the harms of facial recognition and biometrics, and witnessed several public presentations of the projects in digital rights events. It was

at one of these events that I saw an experiment play out with CV Dazzle, which became the third project featured in Chapter 5.

As my analysis progressed from 2017–2019, I scoped out five thematically organized chapters that would address a range of issues identified by respondents while allowing me to inductively develop my theoretical analysis of the material. As already mentioned, my thematic analyses first emerged from a preliminary stage of interviews and participant observation, which aimed to identify prevailing concerns and priorities within the transnational society field focused on addressing the harms of surveillance. Though the chapters are united in their focus on the anticipatory logics and practices involved in civil society's responses to surveillance and related digital threats, each chapter has a slightly different **unit of analysis.** Here I list these units of analysis: **Chapter 4** surveys different threat modelling and risk assessment practices to trace how they have emerged in response to a need to contextualize surveillance uncertainties. This chapter's unit of analysis is **anticipatory practices and their mobility and frictions** as they 'travel' from different sectors into the practices of digital security actors working with NGOs and grassroots groups in support of human rights and social justice movements concerned with surveillance. **Chapter 5** seeks to understand how problem definitions evolved over time within civil society in response to threats. The chapter investigates civil society's priorities as they shift from digital security to corporate data exploitation, and finally from algorithmic discrimination to AI-driven facial recognition. In terms of units of analysis, the chapter studies **three software projects** that exemplify the quickly shifting problem definitions that shape civil society responses to surveillance and datafication amongst security specialists, technologists, and anti-surveillance advocates

Chapter 6 deepens the study of anticipatory practices introduced in Chapter 4 by exploring the enactment of one kind of anticipatory practice within a digital security training. The unit of analysis in question is the **enactment of the practice by a group of people** in a digital security

training. **Chapter 7** brings the focus of the thesis to the role of anticipation in processes of security infra-structuring, looking at the politics of designing and working across information infrastructures meant to facilitate the collective anticipation of threats. Its unit of analysis is **anticipatory security infrastructures.** Finally, **Chapter 8** investigates anticipation as embodied through an expressed imperative by interviewees to act 'proactively'. Its unit of analysis is the notion of **proactivity** as it arises in **two contexts of work to counter and mitigate the harms of preemptive surveillance.**

Research ethics: the DATACTIVE framework & its application to the thesis

My research fell under the ethics protocols of the DATACTIVE ERC project. These ethics protocols were a product of collaborative thinking with Stefania Milan, the outcome of which we set out in three venues: first, a book chapter co-written by several of us in the edited volume *Data for the Social Good*, in which my contribution was to lay out a series of ethical considerations guiding our research (Kazansky et al., 2019). Second, following a period of requirements setting in collaboration with DATACTIVE members and the internal ethics board of the project, Stefania Milan and I put together an unpublished research ethics working paper. Third, Stefania Milan and I made a contribution to a 'forum' in International Studies Perspectives (Tanczer et al., 2020) with a summary of our approach to 'privacy aware research'.

During the first two years of the DATACTIVE project, I helped organize a series of meetings to set out an appropriate approach to our communications, fieldwork and data handling, with a particular emphasis

on privacy, security, and data anonymization. I drew on my expertise in risk assessment (see: Kazansky, 2016) to help us collectively brainstorm these considerations. To kick off this process, I established a set of scenarios for how the lifecycle of collection and dissemination of data might take place, noting points along the research process at which privacy and security concerns might arise. The team discussed contingencies that might arise during situations such as fieldwork trips and travel. We honed in on different data storage and communication needs and then discussed possible tools that would meet them. Together, we developed an information management strategy to prioritize the anonymity, privacy, and security of researchers, informants, research documents, and research outputs. An intensive data protection and anonymization protocol was followed to protect research data throughout the data collection cycle, elements of which are detailed in a separate peer-reviewed article (Tanczer et al., 2020). As part of this, we implemented an internal communication protocol requiring members to use encrypted, secure communications and storage solutions to store data, share data, communicate findings, and plan details of fieldwork. For example, the team used the Signal messaging application for planning on the go, and GPG encrypted email to communicate sensitive details or data. The team also used GPG encryption to store data.

Communicating the goals of the project was a priority to establish trust with participants. For first contact with research participants, we prepared a research statement outlining the aims and methods of the DATACTIVE project, our ethical commitments, and our data security protocols, which we also published on a website that we directed invited research participants to. When possible, we wrote to prospective research participants using PGP encryption or attached our GPG keys in emails as an invitation, though we made sure to use encrypted communications only in cases where we knew ahead of time that it would not present a legal problem related to local information controls. Consent forms were distributed and discussed before the start of interviews. Participants were,

however, offered the opportunity to discuss the consent forms in case they had any special requests regarding data anonymization or redaction. After this period, participants were allowed to retract their participation at any time.

Our research statement and consent forms were reviewed by the ethics board of the DATACTIVE research group. Research participants receiving focused attention within textual outputs of the thesis were provided a chance to review and respond to them before their publication. For reasons of safety and anonymity, the names of informants cited throughout the thesis, along with the organizations and countries they work in, have mostly been anonymised. Their identifying details were replaced with codes, except in cases in which I was given explicit permission to use names, and this was also deemed necessary to properly convey the research findings. The PI of the project kept a physical log of all interviewees and their corresponding codes. Together with the transcripts of the interviews, they were stored at a secure offline location. These documents are to be destroyed at a time in accordance with terms agreed on between DATACTIVE and the ERC. Though interviewees and organizations were mostly kept anonymous, I sought out instances in which it would be possible and appropriate to reference publicly available writing, so that ideas could be attributed back to individuals and groups and textually placed on equal footage with the academic knowledge cited throughout.

Conclusion

This chapter has set out my thesis research design. In the first section of the chapter, I explained my critically engaged research approach and how it informs my data collection and analysis. Next, I explained how I constructed and bounded my research sites following a multi-sited

ethnographic approach to research. Following, I discussed my data collection strategies, including how I organized and conducted interviews, participant observation, and document analysis. I also discussed in detail who I interviewed where I conducted participant observation, and what sorts of documents I analysed and why. Next, I explained the course of my research trajectory, focusing on the many different stages of analysis involved in the development of the thematic analyses featured in the five core chapters of the thesis. Finally, I provided an overview of my ethics protocols. The chapter that follows is the first of the five core chapters of the thesis.