What harms may come?

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

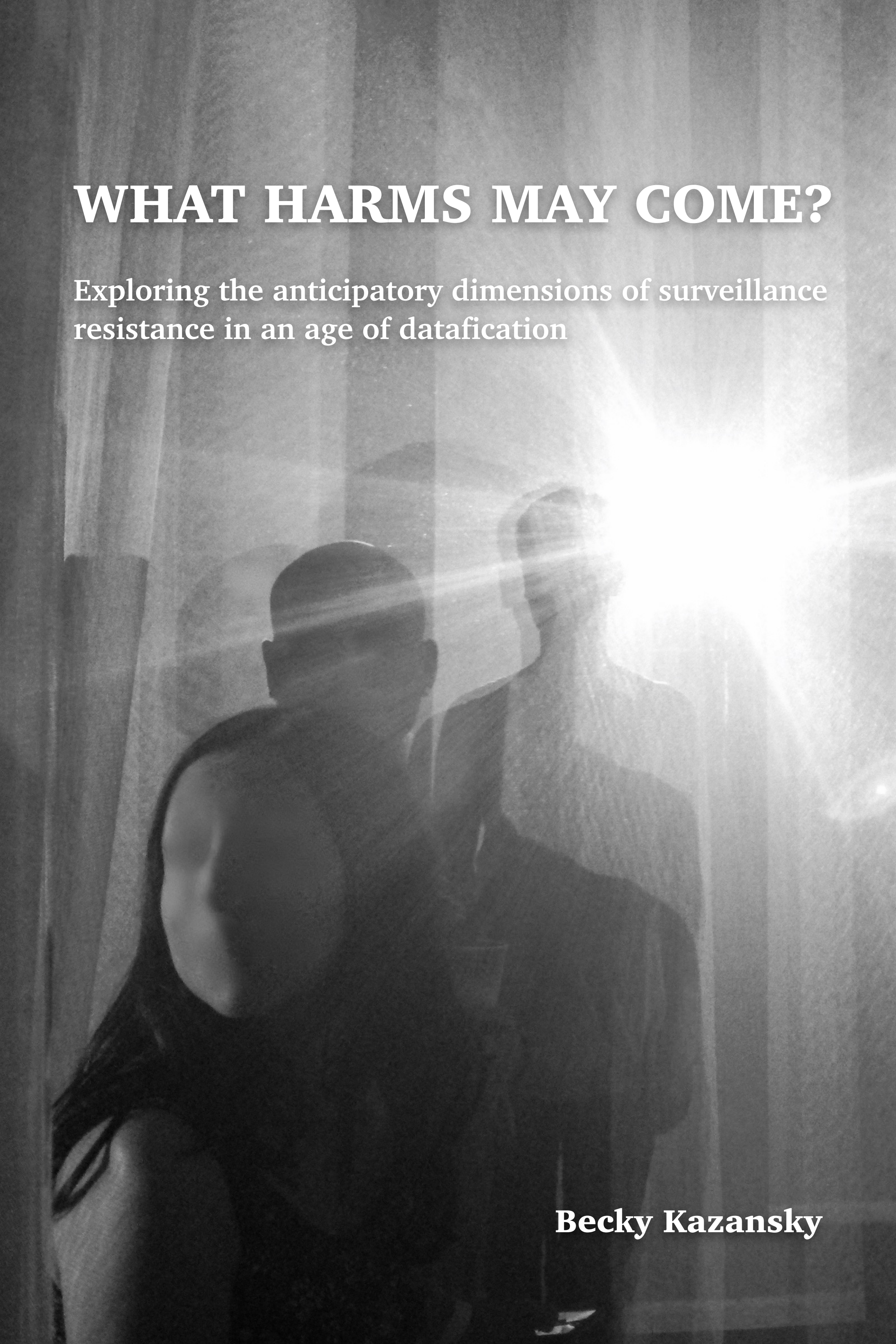
Kazansky, B.

Publication date
2021

Document Version
Final published version

WHAT HARMS MAY COME?

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



Becky Kazansky

What harms may come?

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

ACADEMISCH PROEFSCHRIFT

ter verkrijging van de graad van doctor

aan de Universiteit van Amsterdam

op gezag van de Rector Magnificus prof. dr. ir. K.I.J. Maex

ten overstaan van een door het College voor Promoties ingestelde commissie,

in het openbaar te verdedigen in de Agnietenkapel

op woensdag 8 december 2021, te 10.00 uur

door Rebecca Kazansky

geboren te Pennsylvania

Promotiecommissie

Promotores:
prof. dr. M. de Goede Universiteit van Amsterdam
dr. S. Milan Universiteit van Amsterdam

Overige leden:
prof. dr. T. Poell Universiteit van Amsterdam
prof. dr. T. Blanke Universiteit van Amsterdam
prof. dr. J.P. Dourish University of California Irvine
dr. L.C. van der Velden Universiteit van Amsterdam
dr. F.S. Gürses Technische Universiteit Delft

Faculteit der Geesteswetenschappen

Funding

The research for/publication of this doctoral thesis received financial assistance from the European Research Council under the European Union’s Horizon 2020 research and innovation program (grant agreement 639379-DATACTIVE)

Summary

What harms may come? Exploring the anticipatory dimensions of surveillance resistance in an age of datafication

In an era of ubiquitous data collection, everyday life is suffused with surveillance. The actions of different individuals and social groups are continuously tracked, sorted, and categorized by states and corporations to predict and govern human behaviour. Despite the growing ubiquity of these processes, they often evade notice until their harms are revealed. For communities targeted for surveillance by states, corporations, and other antagonistic actors, how to find safety amidst the consequent uncertainties of surveillance presents an ongoing dilemma. To address the uncertainties, threats, and harms of surveillance, civil society actors working beyond the state and corporate realm come together through transnational collaborations to brainstorm how to anticipate probable surveillance and mitigate its harms. A number of different practices and infrastructures emerge from their activities, which serve to 'tame' surveillance uncertainties, block surveillance, and bring order to the mess of data that pervades contemporary life. Yet the politics of how to resist surveillance are fraught. Understanding how to act amidst presumed surveillance and resulting harms such as harassment, violence, and discrimination, is continuously contested. This thesis delves into the politics and practices of contemporary resistance to surveillance in an era of societal datafication. Its overarching research question is: how does transnational civil society grapple with the uncertainties of contemporary surveillance-related threats and harms?

This thesis explores the temporal and affective dimensions of life under continued threat from actors and institutions that direct biometric surveillance, targeted digital intrusions, preemptive policing, and a milieu of other techniques against the interests of civil society actors concerned

with human rights and social justice. In it, I investigate how a transnationally coordinating 'ecology' (c.f. Star and Griesemer, 1989) of individuals and groups with varying degrees of institutionalization and differing politics make sense of these different forms of surveillance, and develop and maintain an evolving repertoire of mitigations. The focus of my thesis is on the future-oriented modes of thought and action that guide the individual and collective pursuit of safety from surveillance and related harms. I explore the 'anticipatory logics' and practices (Anderson, 2007; 2010) at play to predict, prevent, and recover from probable surveillance threats and related harms. These logics and practices are considered in the context of activities such as risk assessment and threat modelling; digital security preparedness exercises and trainings; security standards-setting processes; and the development of information-sharing infrastructures. By studying the anticipatory dimensions of these activities, I trace how anticipatory logics such as risk, preemption, and prevention travel across different social realms, from areas such as finance and the military into civil society. In tracing how anticipatory logics travel, I explore how civil society actors appropriate and reconfigure these logics within their practices in order to reflect human rights and social justice values. This thesis employs a critical lens on the consequences of life shaped around the need to anticipate surveillance-related threats. I look at how anticipatory practices create new commitments and responsibilities for targeted communities, and how certain practices meant to foster safety may serve to enact political closures and narrowed futures.

This thesis is in conversation with four overlapping fields of study of surveillance, security, data, and society: surveillance studies, science and technology studies (STS), critical security studies, and critical data studies. It contributes to these fields by enriching the study of human agency in a datafied society, and expanding an interdisciplinary understanding of anticipatory logics and practices in the context of surveillance and resistance to surveillance. Empirical data for this thesis is drawn from 50 semi-structured interviews with security specialists, technologists, educators, and affected communities based in 26 countries in different regions of the world, and from participant observation conducted at 12 international digital rights, Internet freedom, digital security, and hacking events in Europe and Southeast Asia. I also include data from a discourse analysis of 120 documents, which describe different techniques related to privacy, digital security, surveillance self-defence, and counter-surveillance.

Samenvatting

Welke schade kan er komen? Onderzoek naar de anticiperende dimensies van weerstand tegen surveillance in een tijdperk van dataficatie

In een tijdperk van alomtegenwoordige gegevensverzameling is het dagelijks leven doordrenkt met surveillance. De acties van verschillende individuen en sociale groepen worden continu gevolgd, gesorteerd en gecategoriseerd door staten en bedrijven om menselijk gedrag te voorspellen en te sturen. Ondanks de groeiende alomtegenwoordigheid van deze processen, ontsnappen ze vaak aan de aandacht totdat hun schade aan het licht komt. Voor gemeenschappen die het doelwit zijn van surveillance door staten, bedrijven en andere antagonistische actoren, vormt het vinden van veiligheid te midden van de daaruit voortvloeiende onzekerheden van surveillance een voortdurend dilemma. Om de onzekerheden, bedreigingen en schade van surveillance aan te pakken, komen maatschappelijke actoren die buiten de staat en het bedrijfsleven werken samen door middel van transnationale samenwerkingen om te brainstormen over hoe men kan anticiperen op waarschijnlijke surveillance en de schade ervan te beperken. Uit hun activiteiten komen een aantal verschillende praktijken en infrastructuren voort die dienen om onzekerheden in de surveillance te 'temmen', bewaking te blokkeren en orde te scheppen in de rommel van gegevens die het hedendaagse leven doordringt. Maar de politiek rondom het weerstaan van surveillance, is beladen. Begrijpen hoe men kan handelen te midden van verondersteld toezicht en de daaruit voortvloeiende schade zoals intimidatie, geweld en discriminatie, wordt voortdurend betwist. Dit proefschrift gaat in op de politiek en praktijken rondom hedendaags verzet tegen surveillance in een tijdperk van maatschappelijke dataficatie. De overkoepelende onderzoeksvraag is: hoe worstelt het transnationale maatschappelijk

middenveld met de onzekerheden van hedendaagse surveillance-gerelateerde bedreigingen en schade?

Dit proefschrift onderzoekt de temporele en affectieve dimensies van het leven dat voortdurend wordt bedreigd door actoren en instellingen die leidinggeven aan biometrische surveillance, gerichte digitale inbraken, preventief politieoptreden en een omgeving van andere technieken die ingaan tegen de belangen van actoren uit het maatschappelijk middenveld die zich bezighouden met mensenrechten en sociale rechtvaardigheid. Daarin onderzoek ik hoe een transnationaal coördinerende 'ecologie' (vgl. Star en Griesemer, 1989) van individuen en groepen met verschillende gradaties van institutionalisering en verschillende politieke overtuigingen, deze verschillende vormen van toezicht begrijpen, en een evoluerend repertoire van mitigaties ontwikkelen en onderhouden. De focus van mijn proefschrift ligt op de toekomstgerichte denk- en handelingswijzen die het individuele en collectieve streven naar veiligheid tegen surveillance en gerelateerde schade leiden. Ik onderzoek de 'anticiperende logica's' en praktijken (Anderson, 2007; 2010) die een rol spelen bij het voorspellen, voorkomen en herstellen van mogelijke surveillancedreigingen en gerelateerde schade. Deze logica's en praktijken worden beschouwd in de context van activiteiten zoals risicobeoordeling en dreigingsmodellering; voorbereidingsoefeningen en trainingen op het gebied van digitale beveiliging; processen voor het vaststellen van beveiligingsnormen; en de ontwikkeling van infrastructuren voor het delen van informatie. Door de anticiperende dimensies van deze activiteiten te bestuderen, traceer ik hoe anticiperende logica's zoals risico, preëmptie en preventie zich door verschillende sociale domeinen verplaatsen, van gebieden zoals financiën en het leger naar het maatschappelijk middenveld. Bij het traceren van hoe anticipatoire logica's reizen, onderzoek ik hoe actoren uit het maatschappelijk middenveld deze logica's toekennen en herconfigureren binnen hun praktijken om mensenrechten en sociale rechtvaardigheidswaarden weer te geven. Dit proefschrift gebruikt een kritische lens op de gevolgen van het leven, gevormd rond de noodzaak om te anticiperen op aan bewaking gerelateerde bedreigingen. Ik kijk naar hoe anticiperende praktijken nieuwe verplichtingen en verantwoordelijkheden creëren voor bepaalde gemeenschappen, en hoe bepaalde praktijken die bedoeld zijn om de veiligheid te bevorderen, kunnen dienen voor het uitsluitend en verminderen van politieke mogelijkheden in de toekomst.

Dit proefschrift is in gesprek met vier overlappende onderzoeksgebieden van surveillance, beveiliging, data en samenleving: surveillancestudies, wetenschaps- en technologiestudies (STS), kritische beveiligingsstudies en kritische datastudies. Het draagt bij aan deze gebieden door de studie van menselijk handelen in een 'datafied' samenleving te verrijken en een interdisciplinair begrip van anticiperende logica's en praktijken in de context van surveillance en weerstand tegen surveillance uit te breiden. Empirische gegevens voor dit proefschrift zijn ontleend aan 50 semigestructureerde interviews met beveiligingsspecialisten, technologen, onderwijzers en getroffen gemeenschappen in 26 landen in verschillende regio's van de wereld, en aan participerende observatie uitgevoerd bij 12 internationale digitale rechten, internetvrijheid, digitale beveiligings- en hackevenementen in Europa en Zuidoost-Azië. Ik neem ook gegevens op uit een discoursanalyse van 120 documenten, waarin verschillende technieken worden beschreven met betrekking tot privacy, digitale veiligheid, zelfverdediging door surveillance en contra-surveillance.

Table of Contents

Acknowledgments

First, I wish to express my immense gratitude to the people who gave their time and energy to sit down for interviews with me, and who trusted me enough to visit their workshops and events as a researcher.

Thank you to my PI and promotor Stefania Milan, who brought me into the DATACTIVE ERC project (grant number 639379) in 2015 at the Media Studies Department of the University of Amsterdam, and to my promotor Marieke de Goede, who embraced my interdisciplinarity and shepherded me into the Transnational Configurations Research Group in the Department of Political Science at the Amsterdam School of Social Sciences. Both have supported me throughout this journey with unfailingly constructive feedback.

Thank you to the University of Amsterdam, and especially to my host institution, the Amsterdam School of Cultural Analysis (ASCA), for providing my project with a home. Thank you to the Amsterdam Institute for Social Science Research (AISSR) for providing me with a joint affiliation and enabling me to participate in PhD training seminars on ethnographic writing with Annemarie Mol. Thank you to Annemarie Mol for introducing me to Kennermerduin Zuid national park and the Dutch NS walking path system, which became my haven over the years. Thank you to the Transnational Configurations Research Group for providing me with financial support to attend two conferences, and thank you to the Young Transcon group, with particular thanks to Barbara Koole and Tasniem Anwar for organizing writing retreats and dinners. Thank you to the Amsterdam Centre for European Studies (ACES) which provided me with financial support for a fieldwork trip.

To my DATACTIVE affiliated comrades & friends: Lonneke van der Velden, paranymphs Niels ten Oever and Guillén Torres, Mahsa Alimardani, Frederike Kaltheuner, Kersti Wissenbach, Jeroen de Vos, Davide Beraldo, Zhen Ye, Jonathan Gray, Sander van Haperen, Fabien Cante and Tomás Dodds Rojas: deep thanks for the exciting discussions, precious feedback and camaraderie during our time together.

To my previous academic home, at ITP NYU: I give thanks for the support provided by my supervisor & institute founder, the late, great Red Burns, and to my fellow students and dear friends Barbra Masters and Greg Dorsainville.

Civil society colleagues & friends: thank you for being co-travellers in thought and action: Eva Blum-Dumontet, Anne Roth, Samir Nassar, Maria Xynou, Alix Dunn, Jeff Deutch, Morana Miljanovic, Claudio Agosti, Daniel O'Clunaigh, Claire Tolan, Hadi Al Khatib, Niko Para, Hannah Smith, Helen Kilbey, Fieke Jansen, Ali Gharavi, Gillo Cutrupi, Gabi Ivens, Azeenarh Mohammed, Leil-Zahra Mortada, Sandra Ljubinkovic, Chinmayi S K, Wojteck Bogusz, Łukasz Krol, Bobby Soriano, Carol Waters, Chris Walker, Kaustubh Srikanth, Zara Rahman and Sandy Ordonez. Thanks to the civil society organizations who took active interest in my research on digital security over the years: HURIDOCS, the Engine Room, Access Now, Greenhost, Witness, the organizers of HackLuxembourg, and the Internet Freedom Festival. Thank you to two of my early professional supporters/former managers from my years working in New York: Jenny Toomey and Micah Sifry.

Co-conspirators and supporters in academe and beyond: thanks go to Seda Gürses for encouraging me to do a PhD; Elinor Carmi, Marianne Franklin, Anita Gohdes, Sarah Myers West, Arne Hintz, Lina Dencik, Ella McPherson, Alice Nah, Julia Slupska and the Critical Security reading group at Royal Holloway for your inspiring scholarship and for inviting me to share my research at various stages in my evolution as a scholar and practitioner. Thank you also to the inspiring scholars who provided feedback on my work at DATACTIVE PhD colloquiums and other DATACTIVE-related events: Linnet Taylor, Annalisa Pelizza, Nishant Shah, Evelyn Ruppert, Ron Deibert, Paul Dourish, Helen Kennedy, and the participants of our Everyday Data workshop in Bremen. Thank you to fellow UvA PhD researchers Natalie Welfens and Anastasiya Halauniova for your incisiveness and solidarity, Elinor Carmi for hosting me on your couch and inspiring me to keep on, Beatrice Martini for knowing just when to check in with RHONY updates, and Sarah Qureshi-Sawyer for friendship found in the middle of a socially isolated pandemic.

Finally, family: thank you to my partner Mischa for Everything; dad Boris and his partner Olga, sister Miriam, brother-in-law Rob, and nephews Jordan and Noah for being family, and parents-in-law Krijn and Marijke for expanding my family. In remembrance, I wish to acknowledge my grandmother Bella and grandfather Simon, who passed in 2017 and 2018 respectively. Finally, I remember my mom Lilia, who succumbed to suicide in 2017. I wish to express my profound thanks to those who stuck by me following her loss, and I extend my solidarity to all survivors of suicide, including the families of the deceased.

Previously published parts of the thesis

- Chapter 4 has been published as a peer-reviewed research article: Kazansky, B (2021) "It depends on your threat model": Understanding the anticipatory dimensions of resistance to datafication". Big Data & Society (8)1, online first (https://doi.org/10.1177/2053951720985557).
- Chapter 5 has been published as a peer-reviewed research article: Kazansky, B & Milan, S (2021) "Bodies not templates: Contesting dominant algorithmic imaginaries". New Media & Society (23)2: 363-381 (https://doi.org/10.1177/1461444820929316). This chapter was co-authored with Dr. Stefania Milan. Both authors contributed equally to the manuscript. While I initially developed the notion of 'counter-imaginaries' and sketched out the theoretical heuristic featured in the chapter, Dr. Milan strengthened these conceptual elements and grounded them in science and technology studies literatures on sociotechnical imaginaries. The empirical data in this chapter is drawn primarily from my thesis field work, with the addition of a focus group conducted by Dr. Milan for the second case featured in the chapter.
- The versions of Chapter 4 and 5 which appear is the thesis are both unaltered in content, other than the removal of acknowledgements, the re-formatting of citations and footnotes, and a change in wording for how I refer to my previously published work in the texts. Where in my published articles, I refer in line to the texts as an 'article', these have been changed to 'chapter'. Where I discuss my own previously published thesis chapters in these two articles through standard citation practices, in the thesis text I cite these by chapter number.

- Chapter 6 has not yet been published, but has been submitted as an article for peer review in July, 2021.
- Chapter 7 has not yet been published, but has been submitted as an article for peer review in July, 2021.
- Finally, Chapter 8 has not yet been published, but has been submitted as an article for peer review in July, 2021.

Abbreviations

AI – artificial intelligence
DDoS – distributed denial of service attack
FLOSS – Free Libre Open Source
HRD – human rights defender
IoT – Internet of things
IT – Information Technology
LAPD – Los Angeles Police Force
LGBTQIA+ - Lesbian Gay Bi Trans Queer Intersex Asexual +
MENA – Middle East North Africa Region
NGO – nongovernmental organization (belonging to civil society)
OS – operating system (computing)
PGP – pretty good privacy encryption protocol for email
STS – Science and Technology Studies
SLSC – Stop LAPD Spying Coalition
US – United States

Chapter 1. Introduction

Introducing the research puzzle

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

'Digital security' is a term held close by civil society's digital security specialists concerned with mitigating the effects of a milieu of threats related to digital monitoring, intrusion, and technologically mediated harassment and violence (Access Now, 2018; Kazansky, 2016; Notley and Hankey, 2013; the Citizen Lab, 2014; the Engine Room, 2013; 2018). In the context of civil society practices, 'digital security' refers to a wide breadth of tools, techniques, and strategies for threat mitigation that are grounded in the daily technology troubles particular to NGOs and grassroots groups. While 'cybersecurity' has become the de-facto term used by states and corporations to frame discussions about technologically related vulnerabilities and recourses against them (Veale and Brown, 2020), civil society actors have long taken pains to extricate security from its state and corporate-centric overtones (Hankey and O'Clunaigh, 2013; Radloff, 2013; 2018). In the context of civil society, many specialists deliberately distance digital security from militaristic notions of security and transplantations of geopolitical sovereignty into digital space. Civil society digital security is also contrasted with narrow, technically focused notions of 'information security' and 'computer security' (Nissenbaum, 2005), fields which, according to the respondents interviewed in this thesis, fail to concern themselves adequately with the human or social dimensions of security. Despite the clear disciplinary notions of civil society digital security, what it constitutes and where its boundaries lie is subject to ongoing negotiation.

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

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

It became clear to everyone seated at the table that it would be impossible to develop a resource able to adequately cover every potential threat for each possible audience. Thus, to scope and structure the curricula, one of the specialists presented the idea that the resource be organized around a heuristic of high, medium, and low risk. The idea was that each user of the learning resource could chose a risk designation that fit their level of danger and targeting, and be led to a cluster of appropriate mitigations, somewhat like a ‘Choose Your Own Adventure’ book. The ‘high risk’ label, the specialist suggested, would refer to people under direct threat. He understood a direct threat as targeted intrusion into a computer, the exfiltration of sensitive information, a campaign of online harassment, or a death threat delivered through the email. The ‘medium risk’ label would refer to users that might feel they are potential targets but lack evidence that they under direct threat. ‘Medium risk’ was seen to map to suspicious events such as a suddenly slow computer, a clicking noise over the telephone wire, a strange car parked in the street outside the office, or a concerning new policy implementation. Finally, ‘low risk’ would refer to users of the learning platform who are engaged in political work but are based in places where rule of law is strong and civil society does its work unencumbered – even if, with every passing year, it has become less and less apparent that such a place truly exists.

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

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

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

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

I want to underscore here that contestations about how to respond to digital surveillance and digital threats are inextricable from the contested dynamics of 'civil society' itself. While many of the specialists described in the opening vignette often imagine themselves belonging to a larger field concerned with fighting for human rights and social justice in the context of technological change and surveillance, this field is highly heterogenous in its aims, politics, contexts, and institutional particularities. In this thesis, 'civil society' broadly refers to the realm of human action beyond the realm of the state and the market (c.f. Gramsci, as explicated in Sassoon, 2000). Narrowing this definition, I use the term civil society to refer to a loose grouping of transnationally coordinating non-profit organizations, grassroots groups, informal coalitions, and individuals working beyond the state and corporations to advance issues at the intersection of human rights, social justice, and technologically related harms. Who considers themselves (or is considered by others) to be part of civil society is subject to continued negotiation. Some groups challenge the very notion of a 'civil society' altogether, instead preferring to talk about their work in terms of community organizing, movement-based work, and radical collectivities.

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

Inspiration for the thesis

Having introduced my research puzzle and discussed the relations and boundaries around some of the important definitions found in this thesis, I now explain how my inspiration for this thesis emerged from my own personal history engaging in civil society work. Since 2009 I have worked as an action-oriented researcher and educator in matters of digital literacy, privacy-enhancing technologies, and digital security (Kazansky 2015; 2016). Over my years in these roles, a recurring question in discussions with other practitioners was how best to break through the uncertainty that comes with determining how to respond as a community to surveillance and data-related harms. In these discussions, I often encountered the common answer that what to do in response to concerns over data and surveillance 'depends on your threat model' — an answer that highlights the contingency and uncertainty at play for individuals seeking safety in a datafied society. I took part in many impassioned discussions amongst security experts and human rights defenders about how to best talk about security risks: should risk be quantified? Is it ethical to frame life around threats and their probability of occurring? Should human rights defenders be made to feel scared to motivate them to protect themselves? Why don't people make use of the security and surveillance countermeasures that exist, and how can they be convinced to change their behaviours in response? These discussions revealed rationalist discourses, patriarchal models of risk communication, master narratives of technological use, and a contentious politics at play in the ways that risks, threats, and the uncertainty of surveillance are conceptualized by 'experts' involved in promoting and developing surveillance and digital security mitigations. As Scoones and Stirling point out, 'addressing uncertainty means confronting inequality, vulnerability, precarity and the deeply embedded inheritances of history head-on. Uncertainty is never just a technical issue' (2020:15). Yet, I found that due to the magnitude of uncertainties and harms many of us tried to address as a field, there was often a compulsion towards trying to 'tame' uncertainty through temporary fixes and heuristics that could provide some small sense of control in the immediate, as also observed by Aouragh et al., (2015). This is not to say that digital security is unnecessary or unimportant. On the contrary.

From 2013–2015 I lead an action-oriented research project that sought to answer how a burgeoning international community of digital security practitioners within civil society could better meet the digital security needs of human rights defenders targeted with surveillance. When this project was first handed to me, its goal was to better promote security 'behaviour change' within communities of human rights defenders. By the end, I had pivoted the project to investigate how structural inequities and political instabilities contributed to human rights defenders' lack of safety, and to what extent the countermeasures promoted by digital security practitioners and technologists helped mitigate them. The project provided an honest reflection on an uncomfortable question. Its main findings were that human rights defenders already put an enormous amount of energy into constructing safety strategies for themselves and their communities. Hence, the problem was not one of motivation or individual behaviour change. Rather, the technologies and pedagogies promoted by civil society organizations to help address issues of digital insecurity often didn’t stand up to their stated purposes (Kazansky, 2015; 2016). The main reasons for this failure included the brittle nature of promoted technologies and a lack of integration of technology concerns with the lived experience of human rights defender communities. This project caused me to reflect on how my practitioner community might contend with risk and uncertainty in more just, ethically, and politically congruous ways.

Formulating the central thesis question

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

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

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

Finally, in studying the future-oriented dimensions of civil society responses to the uncertainties and harms of contemporary surveillance, I note that my research is not simply concerned with 'futures'. Rather, I continuously examine the tension between persistent problems and speculative concerns about possible future threats, looking at how this tension gives rise to particular orientations towards the future. I argue that keeping this multi-temporal grounding is important, considering how much attention has recently been placed both within academia and civil society on the risks of 'high' technologies, such as recent advancements with artificial intelligence. Even as debates rage on about the future of artificial intelligence systems and their promised imbrication into all facets of life, many people at the front lines of human rights and social justice work remain busy with old but deeply entrenched problems tied to resource constraints and the labour of maintaining existing infrastructures. Such problems include not being able to afford trusted IT support, struggles with unreliable privacy enhancing technologies, and powerful and persistent adversaries that remain one step ahead even when 'sophisticated' measures are taken to defend against surveillance and profiling. Amidst this shifting landscape, civil society actors are effectively asked to balance immediate problems caused by persistent constraints with concern over the threatening promise of emerging technologies for surveillance. As advanced surveillance technologies increasingly become embedded into everyday infrastructures and data-driven technologies pervade everyday life, civil society actors wonder what strategies for privacy, security and autonomy will be effective in the coming years. My thesis hence endeavours to look behind and ahead, conceptualizing sticky, persistent problems and peripheral futures within a single topology.

Interdisciplinarity & contributions

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

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

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

Third, the thesis draws from the field of **critical security studies** to examine how anticipatory logics generate particular political possibilities and cause foreclosures (c.f. Anderson, 2007; Amoore, 2013). This field of study offers a rich theoretical base for understanding risk and threat construction as socio-political processes. I apply the field's understanding of risk as a processual and intersubjective phenomenon towards my empirical study of risks and threats in the context of digital security and resistant practices. I build on and contribute to this literature by applying its rich understanding of the anticipatory logics of state and corporate security actors towards a novel purpose: I take the study of anticipation beyond the state and corporate contexts and into civil society.

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

Structure of thesis and methods of data collection and analysis

This thesis takes shape in the form of a multi-sited ethnographic study of surveillance resistant practices and infrastructures. It draws on data collected from 50 semi-structured interviews, participant observation at 12 conferences and workshops in Europe and Southeast Asia, and the close reading of civil society texts on surveillance self-defence, digital security, and cybersecurity. The five core chapters of the thesis, starting from Chapter 4 to Chapter 8, are derived from a reflexive thematic analysis of the data. This method is based on an inductive approach to analysis that surfaces themes from the data and facilitates inductive theory production, rather than already imposing theoretical frameworks onto the data in advance. I discuss my methods of data collection and analysis in more detail in Chapter 3, where I outline my research design.

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

Central themes of the thesis

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

Anticipatory logics: The central theme of study in my thesis is the anticipatory logics that shape the work of responding to surveillance-related uncertainties, threats, and harms. In this thesis, I conceptualize anticipation as the future-oriented dimension of practices and infrastructures that resist surveillance. Under the umbrella of 'anticipation' I include varied state, commercial, and civil society practices shaped by logics of risk, preemption, prediction, prevention, and resilience, among others. While these anticipatory logics are distinct, they are also characterized by their conceptual slippage and mobility throughout different social realms. In my thesis, I trace the mobility and contextuality of anticipatory logics as they are appropriated and reconfigured within civil society practices. Not only do I look at how civil society appropriates and reconfigures anticipatory logics through resistant practices, I also seek to understand how the anticipatory logics of state and corporate actors violently clash with those of civil society actors.

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

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

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

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

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

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

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

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

Thesis Chapters overview

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

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

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

While Chapter 4 surveys anticipatory data practices in the context of civil society digital security, in Chapter 6, I look in more depth into the enactment of risk assessment, exploring it within the particular context of ta digital security training organized for human rights defenders. Titled: Taming uncertainty into risk: towards a critical lens on risk management practices in digital and cyber security', this chapter introduces the concept of ‘qualculative convergence’ to describe the intersubjective process that transforms unwieldy uncertainty into formalised digital security risk. With this concept, I make a critical intervention into enterprise risk and security tropes, challenging rationalist and behaviouralist discourses common for commercial and state cybersecurity by demonstrating the ‘messy’ forms of collective valuation that go into the construction of a risk as such. Through this ethnographic exploration of a digital security training, I show how digital security trainings facilitate the transformation of uncertainty into risk, and how the training culminates in convergence around an appropriate path of action to counter surveillance and digital harms.

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

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

Conclusion

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

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.

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.

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

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

Abstract

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

Introduction

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

Challenging the idea that people have succumbed to ‘digital resignation’ (Draper and Turow, 2019), a multitude of potential tactics are marshalled to cope with the ‘mess’ of data and digital life (Pink et al., 2018) and counter ‘imagined surveillance’ (Duffy and Chan, 2018). People disclose information selectively to certain parties (Marwick and boyd, 2014);‘back up’, guard and duplicate important information (Pink et al., 2018); engage in ‘vernacular resistance’ through obfuscation (Brunton and Nissenbaum, 2015) and create new technologies to shield against tracking and profiling (Kazansky and Milan, Forthcoming; Milan and Van der Velden, 2016). For targeted groups and populations, the high stakes of surveillance ‘discovery’ (Marx, 2009) has resulted in a continuous adaptation of practice (Kaun and Treré, 2018). Techniques of resistance must stay abreast of techniques of surveillance (Leistert, 2012). However, despite their constant adaptation, resistant tactics and strategies do not necessarily succeed in their goals (cf. Brunton and Nissenbaum, 2015). As Hong (2015) points out, amidst the unknowns of surveillance, counter-measures might instead only provide a ‘simulation of safety’(70). How exactly to act and adapt – in other words, which tactics and strategies will bring desired effects in unstable and contingent situations – is thus subject to continuous controversy (Musiani and Ermoshina, 2017). The question of what constitutes an ‘effective’ tactic to resist surveillance and counter data harms is one of ongoing inquiry both in academic literatures and across social movements (Aouragh et al., 2015; Dencik et al., 2016; Gürses et al., 2016; Monahan, 2006).

Responding to an interdisciplinary imperative to deepen understandings of resistance and agency amidst datafication (Couldry and Powell, 2014; Kennedy et al., 2015), this chapter explores two related practices enacted by affected communities to fight digital resignation and facilitate agency: ‘threat modelling’ and ‘risk assessment’. These interrelated practices sit within a larger cluster of what I term ‘anticipatory data practices’. Concerned with determining the likelihood of imagined potential surveillance-related harms, anticipatory data practices take up the task of untangling data ‘mess’ and ‘cobbling what we know and suspect into a picture of a sensible, working world’ (Hong, 2015: 73). Through structured, future-oriented modes of sensemaking, they serve to tame the uncertainties of contemporary surveillance, turning political strife and unpredictable danger into a ‘manageable’ problem. In recent years, several scholars have highlighted the prevalence of practices such as threat modelling and risk assessment amongst technologists and activists concerned with digital security and surveillance counter-measures. Ermoshina and Musiani (2018) characterise threat modelling and risk assessment as ‘powerful instruments to narrow down and structure’ interventions intended to bolster security and safety for activists (p. 32). Myers West (2017) highlights the 'extensive time and energy' spent by civil society groups 'building threat models, and calibrating their activities in response'. Through a multi-year study, this chapter delves deeper into these important practices, exploring how their 'anticipatory logics' (Anderson, 2007, 2010) enable digital security specialists and civil society groups to cope with surveillance-related uncertainties. The chapter also interrogates the political commitments these practices create through their focus on future-oriented modes of action. In so doing, the chapter brings into dialogue contemporary literatures on anticipation with studies of activism, resistance and data practices, aiming to advance a critical perspective on resistance and agency in times of datafication.

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

Situating anticipation

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

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

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

Methods

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

Interviewees were based in a total of 26 countries from across different regions of the world. Their diffuse geographical representation resulted from the transnational patterns of coordination common for civil society projects concerned with digital issues such as Internet freedom, counter-surveillance and digital rights (Myers West, 2017). A number of interviews were conducted at the site of their international meeting points. Interviewees were selected for their contributions to counter-surveillance practices as educators, technologists and representatives of surveillance-affected communities. They were asked to reflect on the changing state of their field and to describe the tactics and strategies they use to identify and counter 'digital' threats. Names and identifying details – including specific organisations, countries and in many cases regions – have been anonymised to respect the sensitive nature of the work documented in this study. Of note, the analysis in this chapter gives outsize space to the perspectives of educators. Fitting under the educator category are people identifying as facilitators and digital security trainers, whose role is to work with affected communities to 'raise awareness' of digital surveillance threats, increase technological literacy and promote particular counter-measures (Ermoshina and Musiani, 2018; Kazansky, 2015).

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

Digital security and digital universalism: Friction and critique

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

Yet these advancements have also produced social frictions (Costanza-Chock et al., 2018). Aouragh et al. (2015) argue that the labour divisions and politics of expertise bound up in the development and promotion of digital surveillance counter-measures have resulted in ‘sneaky moments’ that reinstate the very hierarchies and structures being fought against. In their analysis of civil society campaigns promoting digitally secure practices, they critique the ‘tendency for tech activists to develop universal technologies with a ‘design from nowhere” (p. 226), which are then positioned as solutions to complex social problems. This ‘design from nowhere’ parallels the ‘digital universalism’ which Chan (2013) finds embedded into dominant discourses and practices of technological development. Educators interviewed for this study critique a resulting expectation that affected communities adopt the use of potentially inappropriate, ‘tool-centric solutions’ (Interview #43). ‘Every technologist you ask, they say, you wanna be secure, just use Tor, use Signal’, joked a digital security trainer referencing the prevalent recommendation in the ‘digital security community’ that those concerned with the confidentiality of their data use these two particularly robust software tools for safer communications (Interview #14). As the trainer pointed out, the use of these tools can in fact increase the vulnerabilities their developers claim to counter. For example, at the time of writing, the Signal chat application requires the disclosure of a personal phone number in order to set up a ‘user account’, data which may expose a person to further surveillance (Shelton, 2018). A number of interviewed trainers and human rights defenders (HRDs) noted in our discussions that Tor, a tool widely used to circumvent censorship, has often ‘failed’ to work for a number of reasons, ranging from efforts by governments to block the tool’s use, to the slow Internet speeds still found across many rural regions of the world. Thus, ‘at best, these approaches typically build skills for particular tools without an ability to adapt’, notes Norman Shamas, an educator proposing to discuss how to ‘create a pedagogy of empowerment’ at a large annual meeting bringing together the international Internet freedom community (Shamas, 2017). With safety a concern, the 2019 edition of the same conference included a workshop by staff of the Electronic Frontier Foundation (EFF) asking ‘How Can We Share Secure Messaging AdviceWithout Causing Harm?’ The session description notes ‘the best choice for one person could be catastrophic for another’ (Li and Trendacosta, 2019).

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

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

From the universal to the contingent: Enter threat modelling

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

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

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

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

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

Assessing risk: Situational awareness versus self-care

Alongside threat modelling, interviewed educators also turn to the closely related practice of ‘risk assessment’ to surface, map and mitigate the concerns of affected communities worked with. Although the burgeoning field of ‘risk assessment’ methodologies has well-documented roots in insurance and financial speculation (Bouk, 2015; Hacking, 1975), the focus in this chapter is on understanding the configuration of risk assessment as it arises in digital security trainings and organisational digital security processes particular to civil society. As I will show, some conventions and discourses persist while morphing to account for the values and goals particular to civil society. A security guide titled the Front Line Defenders (2011) Workbook on Security offers a conceptual window onto risk assessment particular to civil society, featuring several chapters devoted to different elements of assessing risk for an intended audience of ‘high-risk’ HRDs. One section in particular focuses on behavioural strategies where surveillance is suspected. Here, the anticipatory elements of the practice are made explicit, with a pedagogical focus built around the assumption that surveillance is more likely than not. ‘Make a plan for how you would deal with this before it happens to you’, the workbook directs (p. 36). It advises that HRDs who suspect they might be under surveillance should ‘assume that you are’ (p. 39). Furthermore, it recommends that HRDs ‘make a list of the actions you will take to deal with the situation’ (p. 37) though it also emphasises that ‘it is important to maintain a balance between taking precautions and not becoming paranoid’ (p. 36). As such, the workbook reflects a fundamental ambivalence towards the notion of ‘awareness’ and vigilance, demonstrating also a sense of resignation to the idea that surveillance is unavoidable.

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

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

A second difference between how threat modelling and risk assessment are framed in civil society texts and exercises is that instead of only focussing on ‘things’ or ‘assets’ that need protection, risk assessment also emphasises the ‘capabilities’ of civil society actors, which, according to one digital security trainer, enables affected communities to see that despite threats and anxieties, they possess agency and power. The relationship between these units of analysis is made plain in a frequently discussed instrument used within the process of risk assessment: a ‘risk equation’. As laid out in a security guide titled the New Protection Manual (Fernandez and Caraj, 2009) by human rights organisation Protection International, the risk equation requires its implementer to identify which people, objects and institutions in their life represent an ‘asset’, ‘capacity’ or ‘vulnerability’. These three categories of people, objects and institutions are then commensurated in order to achieve a measure of risk, where ‘risk = threats × vulnerabilities/capacities’. The process of valuation may produce a numerical figure representing the ‘level’ of risk at hand, which is then mapped to a set of potential actions meant to mitigate the risk. In other cases, the notion of ‘risk’ remains qualitative. The question of whether to apply quantifying or ‘numbering’ methodologies within risk assessment was a sticking point for the digital security trainers interviewed. Some frameworks of civil society risk assessment disavow the quantitative valuation of lived experience. One interviewed digital security trainer believed quantification to be alienating, questioning, ‘how do you not get lost in the formula?’ (Interview #15). A second trainer similarly argued that ‘using statistics on a single person is not intuitive’ (Interview #10). Yet others interviewed believe numbers bring an essential feeling of tangibility to a situation that can otherwise remain in the abstract: ‘Having numbers or figures or scales as to how dangerous or not dangerous stuff is heightens the sense of importance’ (Interview #6). This proponent of calculative techniques acknowledges that though quantitative analysis ‘can be a source of stress’ it ‘really pushes the change that you need’.

The risk equation featured in the New Protection Manual provides an example of the way anticipatory logics and practices travel and transform across social worlds, with educators importing anticipatory conventions from other sectors concerned with risk and threat management, and enrolling those they work with into their logics in order to ‘push’ ‘needed’ changes to the practices of affected communities. As already mentioned in the section on threat modelling practices, it is possible to trace how educators themselves are enrolled into anticipatory logics. Whereas threat modelling practices were said to be brought into civil society through collaboration with engineers, digital security trainers describe a different origin for their risk assessment methodologies. In interviews, several digital security trainers noted that the risk management protocols followed by their organisations were first established by former military personnel who had served as private contractors in conflict zones, before moving into civil society communities concerned with digital rights and Internet freedom. In the humanitarian field, risk management has been a highly institutionalised process going back to the 1990s (Duffield, 2010). While the predominant focus of risk assessments in the humanitarian field was traditionally on the physical and ‘operational’ dimensions of security in conflict zones, as digital technologies have became pervasive, digital information management has become an increasingly important component of a broader risk management strategy. The pre-eminence of digital concerns created an imperative to merge multiple streams of security work into one, a project which has since 2011 been carried forward by a community of digital security trainers working with HRDs and digital rights activists to develop a ‘Holistic Security’ methodology (Tactical Technology Collective, 2016).

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

As a further step in their feminist re-orientation of security, Holistic proponents set forth a care-oriented definition of security as ‘wellbeing in action’ (Tactical Technology Collective, 2016: 21). Care, in this context, means to reject fear of abstract threats and to instead embrace what is immanent and felt. Through its distancing from totalising conceptualisations of surveillance, the methodology tempers the militaristic compulsion to continuously engage in vigilant threat identification processes. However, the methodology still demands vigilance, to a degree. For example, as part of a process of ‘Holistic risk assessment’, the Holistic Security Manual requests that the individual engage in the continued, daily analysis of potentially concerning security events in order to gain an 'accurate picture' of security (p. 59). The strong suggestion that individuals maintain awareness of potential threats, together with a rationalist focus on accuracy, demands that affected communities engage in an intensive form of anticipatory labour. This labour risks reproducing the very overwhelm which the methodology tries to mitigate (cf. Harvey et al., 2012).

From digital security to data politics: Consequences and conclusions

As concerns with surveillance and datafication have increasingly shaped the work of transnational civil society, civil society has turned to practices which aim to structure and tame the 'mess' of data. As this chapter has shown, anticipatory data practices such as threat modelling and risk assessment serve to guide action amidst the uncertainties of surveillance and data exploitation, weighing the likelihood of imagined potential future data harms, articulating situational contingencies and mapping these contingencies to appropriate counter-actions. Anticipatory data practices thus function as a heuristic aid for choosing other practices and 'tools' to counter concerns over surveillance and datafication. This process of heuristic-making takes place through the structured operationalisation of anticipatory logics. Importantly, this chapter has shown that in spreading and promoting anticipatory data practices, technologists and educators enrol surveillance-affected communities into anticipatory modes of doing and being, demonstrating the way that anticipatory orientations towards the future spread throughout civil society practices concerned with safety and counter-surveillance. My findings further show that a diverse array of conventions, practices and values are imbricated within anticipatory data practices, strengthening the assertions by Pink et al. (2018) that ‘there is no single template, logic or set of principles that is universally followed’ for coping with the ‘mess’ of data (p. 12). Yet, while the lack of universal ‘solutions’ to the mess of data and digital life is certainly also a central theme here, this chapter shows that anticipatory data practices are emblematic of the urgent labour by civil society actors to bring structure to the ‘mess’. In other words, the idea that how to respond to surveillance and datafication ‘depends on your threat model’ can be understood as an attempt to find an anchor amidst the overwhelm of contemporary data mess. Hence, the value of threat modelling and risk assessment practices is in the clarity and simplification they can provide.

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

In response to these critical questions, it is important to highlight that the preoccupation with practical fixes and ‘anticipatory modes’ of action within civil society is not uncritical or naive. First, many interviewees acknowledge that no matter how robust a privacy-enhancing technology or digital security tool, there is no single solution for ‘defence’ amidst the many worries that come with contemporary modes of surveillance. ‘Datafication is the kind of thing that you can’t solve with security tools’ one activist digital security tool developer admitted (Interview #26). Furthermore, interviewees describe a growing focus on connecting work on daily tactics with broader social critiques and issues of ‘data politics’ (c.f Ruppert and Bigo, 2017). An interviewed digital security trainer from a group supporting ‘self-defence’ in European labour unions reflected on the fact that while the work of the group began with promoting a set of particular set of digital security tools, their work has gradually shifted towards the political interrogation of datafication:

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

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

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

While his remark seems to signal a sense of resignation (per Draper and Turow, 2019), the trainer plans to continue his quest for practical counter-measures out of a belief that new footholds for resistance and agency are always emergent. Building on this belief, another digital security trainer argued that while self-defence might be a limiting frame for political mobilisation, ‘for people who are in danger…that danger can’t wait for you to impact public policy' (Interview # 41). He thus further emphasises that practical fixes and daily tactics have a role to play in broader strategies aimed at achieving structural changes. Meanwhile, his concern with everyday safety highlights that the 'digital security ecosystem' (the Engine Room, 2018) of civil society is engaged not just in 'acts of symbolic resistance' (per Monahan, 2006: 516) but is fundamentally concerned with the daily survival of civil society and social movements more broadly.

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

Chapter 5. “Bodies not templates”: Contesting dominant algorithmic imaginaries[8]

8 This chapter has been published as a peer-reviewed research article: **Kazansky, B** & Milan, S (2021) “Bodies not templates: Contesting dominant algorithmic imaginaries”. *New Media & Society (23)2:* 363-381. . It has been co-authored with Stefania Milan, PI of the DATACTIVE ERC project. Both authors contributed equally to the manuscript. The data in this chapter is drawn primarily from my individual thesis project (the data of which is part of the collectively stewarded DATACTIVE corpus of interviews), with the addition of a focus group conducted by Stefania Milan for the second case featured in the chapter. The version of Chapter 5 which appears here is unaltered in content, other than the removal of acknowledgements, the re-formatting of citations and footnotes, and a change in wording for how I refer to my previously published work in the texts. Where in my published articles, I refer in line to the texts as an ‘article’, these have been changed to ‘chapter’. Where I discuss my own previously published thesis chapters in these two articles through standard citation practices, in the thesis text I cite these by chapter number.

Abstract

Through an array of technological solutions and awareness-raising initiatives, civil society mobilizes against an onslaught of surveillance threats. What alternative values, practices, and tactics emerge from the grassroots which point toward other ways of being in the datafied society? Conversing with critical data studies, science and technology studies, and surveillance studies, this chapter looks at how dominant imaginaries of datafication are reconfigured and responded to by groups of people dealing directly with their harms and risks. Building on practitioner interviews and participant observation in digital rights events and surveying projects intervening in three critical technological issues of our time—the challenges of digitally secure computing, the Internet of Things, and the threat of widespread facial recognition—this chapter investigates social justice activists, human rights defenders, and progressive technologists as they try to flip dominant algorithmic imaginaries. In so doing, the chapter contributes to our understanding of how individuals and social groups make sense of the challenges of datafication from the bottom-up.

Introduction

The datafication of social life has altered the relation of individuals and communities with their surroundings. The blanket monitoring of citizens has fostered the emergence of a diffuse culture of surveillance, whereby surveillance has been domesticated and naturalized (Lyon, 2017). Most appear to have accepted the matter-of-fact data exploitation enacted by states and corporations alike, to the point that it has become arduous to imagine possible alternatives (Dencik and Cable, 2017; Draper and Turow, 2019). Amid this background, however, portions of the citizenry are trying to subvert dominant practices and perceptions of datafication, instilling critical questions into the public discourse and offering technical interventions to counter surveillance. Civil society[9] has long been concerned with developing alternative visions and practices in response to technology related harms (see for example, De Filippi and Treguer, 2014; Kubitschko, 2015; Musiani, 2016). Civil society actors have sought to "pour as much sand into this machine of suspicion as we possibly can" (Milan, 2013: 156), engaging in subversive or defensive individual practices, civil disobedience against unfair laws, policy advocacy and the creation of resistant infrastructure (cf. Aouragh et al., 2015). The ubiquity and extraordinary pervasiveness of datafication, however, presents today's activists with ever-newer challenges. One of the challenges of responding to the societal effects of datafication is the complexity and rapid pace of change in its sociotechnical arrangements, which create a shifting milieu of threats. This "threat landscape" requires civil society to continuously adapt its repertoire of tactics in response (cf. Kaun and Treré, 2018), producing a churn of ideas, mobilizations, values, and symbols to make sense of their social worlds. Conversing with the disciplines of critical

9 The umbrella term "civil society" identifies the realm of human action beyond the state and the market: a diverse group where distinct visions and values co-exist, not without frictions. It includes nongovernmental organizations, informal coalitions and groupings, and concerned individuals.

data studies, science and technology studies (STS) and surveillance studies, this chapter takes the continuous evolution of civil society responses as a subject of study. Looking at the interplay between emergent imaginaries and practices in the shifting tactics of resistance to datafication, it asks how people variably affected by the harms of datafication and surveillance seek to make sense of technological change and respond to the injustices harboured.

Through a qualitative analysis of interviews, documents, and events, this chapter investigates how civil society actors counter the evolving threats of datafication through technological interventions. We use the notion of "imaginary" applied to technology (see for example, Wyatt, 2004) to capture the visions and values subtending to these grassroots practices, which form an integral part of the action repertoires of contemporary movements. We can understand imaginaries as the outcome of individual and collective sense-making activities resulting in shared ideas about technology, including fears, hopes, and expectations. We observe civil society actors as they re-appropriate and subvert the dominant imaginary of technological innovation, societal benefit, and inevitability of surveillance set forth by what has been termed the "surveillance-industrial complex" (Ball and Snider, 2013). These contestations produce what we call "counter-imaginaries" that interpret the needs and/or serve the interests of affected social groups. These counter-imaginaries make apparent how civil society seeks to respond to the ever-complex technological change and the risks it conceals.
We explore emerging counter-imaginaries of datafication as they are enacted within three open-source[10] software projects. These projects intervene in three crucial sociotechnical problems arising with datafication, specifically, the breaking of the "endpoint security" of computers by state actors and its impact upon human rights advocates and

10 Free/libre open-source software (FLOSS) indicates software for which the source code is shared to encourage people to customize and ameliorate its functionalities.

other vulnerable populations; the perils of an always-on and pervasive Internet of Things (IoT); and the advancement and diffusion of "smart" data-driven surveillance, as seen with advanced biometrics and facial recognition systems. First, we look at an innovative operating system (OS) called Qubes, aiming to put digital security at the center of its design considerations. Next, we examine Dowse, a device which makes explicit the complex data flows of IoT home appliances and for this reason is presented by its developers as "the Internet of Things missing On-Off button." Finally, we observe the activist appropriation of an artistic project called CV Dazzle, which plays with facial camouflage in response to the threat of automated "face surveillance." These three areas of intervention, we argue, sit at important junctures in civil society practice. They are paradigmatic of how the evolution of problems and priorities lead civil society to adapt their practices through new tools, infrastructures, and approaches. By looking at how grassroots practices evolve in response to technological threats, the chapter contributes to our understanding of how different social groups make sense of datafication (Couldry and Powell, 2014; Kennedy et al., 2015; Milan, 2018). In particular, it sheds light on ways to understand resistance amid concerns with increasingly pervasive surveillance, automation, and artificial intelligence (AI) highlighting how social actors problematize mainstream notions of technological progress. First, we first describe our empirical material. Second, we contextualize imaginaries in the midst of civil society responses to datafication. Third, we present our analytical lens for understanding how counter-imaginaries are co-produced and evolve amid shifting material and social arrangements and priorities. To this end, we identify three "phases of response" in civil society's attempts at making sense of the treats of datafication. We then analyse our cases, which reflect these shifting arrangements and priorities, exploring the subtending counter-imaginaries.

Methods

We identify civil society counter-imaginaries in the narratives, tools and practices social actors engage with when seeking to counter the threats of datafication through open-source software projects. Our case studies, which reflect widely discussed ideas and ambitions with the civil society realm, have emerged out of a multi-year observation of digital rights, Internet freedom, and radical tech communities.[11] Data for this chapter, in particular, derive from a multi-sited software ethnography (Star, 1999), combining the discourse analysis of technical documentation with fieldwork notes and semi-structured interviews. Technical project documentation analysed included white papers, user guides, and websites in order to trace technical changes and shifting project priorities. Participant observation (2016–2019) took place at six sites across Europe, ranging from hacker space "meetups" to workshops at large conferences. For the Qubes case, we attended a workshop designed to help the 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. For Dowse, we joined a meetup of tinkerers intervening into IoT, featuring a tool demonstration, and involved its core developers in a focus group. For the CV Dazzle case, we participated in a workshop about how to raise awareness and counter the harms of facial recognition and biometrics. We also attended public presentations of the projects in digital rights events. We complemented these observations with in-depth interviews with developers and maintainers of software infrastructures, as well as representatives from frontline communities engaged in human rights and social justice work and seeking to make use of the projects of study. The semi-structured interviews were designed to

11 At the time of writing, our dataset included, for example, about 250 semi-structured interviews with individuals and organizations engaging with datafication by means of policy advocacy, data literacy and campaigning, and tech development (https://data-activism.net).

identify areas of concern and to facilitate discussion of values and practices. Next, we situate the notion of “imaginary” in the literature.

Counter-imaginaries of datafication

If “social imagination is a key process in all social life” (Schinkel, 2017: 6), technology constitutes today the digital backbone of such imagination —and a central concern for our imaginative faculties. Social movements have traditionally been the bearers and custodians of alternative imaginaries of radical change (cf. Fotopoulou, 2014; Smith, 2012). Similarly, the actors addressed here seek to produce imaginaries pointing to different ways of being in the datafied society. But what are imaginaries and why do they constitute a useful lens to understand the evolution of civil society “thinking and doing” about the threats of datafication? Imaginaries point to collective, shared visions about technology, which amalgamate “intentions and projects as well as utopias and ideologies” (Flichy, 2007: 4). As a mechanism of “social-representation” (Castoriadis, 2005: 247), they allow users to “think about what infrastructures are, where they are located, who controls them, and what they do” (Parks, 2015: 355), especially when infrastructure is invisible and its functioning largely unintelligible to end users. According to Verran (1998), imaginaries emerge from mundane, situated epistemic practices. Furthermore, in the STS tradition, they are understood as being entwined with the socio-material practices of technological use and development. They emerge from “the imaginative faculties, cultural preferences and economic or political resources” of users (Jasanoff, 2004: 16). They are co-produced by varied actors with different values, modus operandi, and agendas (see for example, Wyatt, 2004). They tend to have a normative function, as they are simultaneously “descriptive of attainable futures and prescriptive of the kinds of futures that ought to be attained” (Jasanoff et al., 2007:1).

Not surprisingly, the notion of imaginaries has gained traction in recent analyses of citizen engagement with datafication and data infrastructure (e.g. Bucher, 2017; Lehtiniemi and Ruckenstein, 2019; Mansell, 2012; Milan and ten Oever, 2017). This is because the notion constitutes a useful framing to understand how individuals and communities make sense of technological change through mundane practices (see Verran, 1998). It also allows us to observe practitioners in action as they attempt to shape their technological present and future. In fact, not only are (algorithmic) imaginaries “productive of different moods and sensations” (Bucher, 2017: 41), they also perform a generative function as “different ways of thinking about what algorithms are and do may affect how these systems are used” (p. 32). Similar to “dominant” imaginaries, which “not only shape what is thinkable but also the practices through which actors perform them” (Ruppert, 2018: 4), the counter-imaginaries analysed here animate civil society’s tactical responses to perceived threats to its values and ways of living. Like the threats they mobilize against, counter-imaginaries are in continuous evolution. Capturing and condensing the users’ rich visions and values, they make apparent complex sense-making activities. They play a key role in making surveillance threats “thinkable” as a step toward identifying responses, thus helping to explain tactical choices and strategies. But they perform also a crucial mobilization function, serving the purpose of making publics (Marres, 2012), rallying groups of people and marshaling resources around counter surveillance. How can we understand these counter-imaginaries and their evolution?

Capturing shifting counter-imaginaries: a heuristic

In the last decade, civil society has increasingly been concerned with digital surveillance. Concerns peaked in 2013 following the Snowden leaks, which exposed the blanket monitoring of citizens by national security agencies and industry collaborators (Hintz and Milan, 2018; Lyon, 2015). In the years since, civil society has engaged in fights for the right to encryption (Hellegren, 2017), against "data exploitation" and around the just application of automated systems (cf. Hintz and Brown, 2017). Amid these developments, affected communities have tried to make sense of risk in their daily practices, continuously assessing their environment, engaging in "threat modelling," and adapting practices accordingly (Myers West, 2017). "Tech activists" (Aouragh et al., 2015; Milan, 2013) and civil society organizations have sought to raise awareness of emerging issues of concern and have developed technological interventions in response (Daskal, 2018; Dencik et al., 2016). These activities have resulted in a plethora of software projects which undergo a continued iteration in response to shifting concerns and priorities. We look at these projects as bearers of civil society counter-imaginaries of datafication.

In an effort to trace how civil society counter-imaginaries take shape amid concerns over datafication, we distinguish three "phases of response" in civil society's technical interventions, namely, "speculative," "formative," and "stabilized." The three phases, to be understood as ideal types, are the result of our prolonged exposure to the field and the analysis of social actors' narratives. While a research outcome on their own, here they are mobilized as a heuristic lens for understanding how civil society responses evolve in relation to ever-changing challenges and priorities. As often the case with ideal types, the boundaries between these "phases of response" are permeable. Furthermore, there is no prescriptive sequence by which they unfold, thus the phases should not necessarily be understood as consecutive. The phases of response are as follows:

(a) A stabilized response refers to a sociotechnical issue that has been identified and analysed as a problem, and "made manageable" through a repertoire of software tools and tactics shared across an allied community. In other words, the problem at hand has been domesticated, with tech "fixes" undergoing development and integration within the practices of social groups affected by the particular problem addressed.[12]

(b) A formative response refers to issues toward which concrete technical interventions are currently in development. A problem has been identified and analysed by social actors but is only at the formative stage of containment through particular repertoires of software tools and tactics.

(c) A speculative response arises in a period of ambivalence: the issue—and its attending problems—must still be made "thinkable," pending the "shifting of the conditions in which [it] might come to make sense" (Gabrys, 2017: 176). Interventions, such as awareness-raising initiatives and digital literacy resources, are thought up and played with to make the issue more tangible for affected communities, but a concrete tech "fix" is at this stage felt to be elusive.

When a response is in its speculative phase, it fulfills a diagnostic function, facilitating the initial identification of problems, causes, and potential harmful consequences. When a response is in its stabilized or formative phases, it performs instead a prognostic function, offering particular interventions for an identified problem.[13] In these latter phases,

12 It is worth noting that it is not the counter-imaginary per se that has been stabilized, as imaginaries are in continuous evolution, but the problem at hand and the related fixes.

13 Social movement scholars adopt a similar distinction when investigating the role of collective action frames in fostering mobilization. A diagnostic

civil society actors converge around expected scenarios and events. “Solutions” such as novel digital practices and resistant infrastructures are developed in anticipation of particular future outcomes (cf. Alvial-Palavicino, 2016).

Using this heuristic, we identified three paradigmatic software projects, namely Qubes, Dowse, and CV Dazzle, whose analysis allows us to observe the emergence of civil society counter-imaginaries. Qubes is a “stabilized” response to the threats of targeted surveillance. While it does not (promise to) solve the root causes of the problem at hand, its developers (and, to lesser extent, users) have established a particular repertoire around self-defined “effectiveness” in relation to a delimited set of digital security threats. Little more than a working prototype, Dowse constitutes a response to the datafication of the consumer lifeworld which is currently in its formative stage. It enacts an imaginary of “awareness” to cope with the ambient threats of data leaks and exfiltration that accompany IoT. Third, activists engage in speculative activity through the use of CV Dazzle in order to raise awareness around the threats of AI and automated surveillance. This artistic project helps to “feel out” a response to looming yet abstract threats. Next, we explore each project and the counter-imaginary it enacts.

Qubes: towards a secure desktop ecosystem

Qubes (qubes-os.org) is an OS structured around the idea of allowing users to create an almost unlimited amount of discrete “safe” spaces from which to conduct their digital life.[14] With a system architecture optimized around providing such spaces, the project seeks to address what Qubes

framing identifies a problem and assigns blame, whereas a prognostic frame proposes solutions to the problem at hand (Snow et al., 1997).

developers identify as a crucial problem plaguing contemporary computing systems—namely that matters of digital security are seen as an "add-on" or left as an afterthought in the development of technical infrastructure. By breaking computing into smaller discreet pieces, Qubes tries to re-envision how an OS looks and works. As explained by a user interviewed for this study, Qubes empowers its users to "create spaces for yourself […] where you feel physically comfortable and can undress from the armor. You don't need to be on the watch all of the time" (Interview #11).

In development since 2009, the founder, Polish computer scientist Joanna Rutkowska, envisioned a system which would contain the many different kinds of attacks that can occur when users connect their computers to a network amid a rapidly evolving "threat landscape" of targeted surveillance and intrusion. Started as a personal project, Qubes has attracted a small paid team and a community of volunteers and users, raising hopes for a new kind of computing experience free from hyper-vigilance (see Harvey et al., 2012).

How does Qubes work? Upon first "logging in" to the OS, the user accesses a standard desktop window. A little "Q" icon on the menu selector gives her access to a list of self-contained "virtual machines" which function as separate, secure spaces within a larger computing environment. Some virtual machines are designated as "disposable"—meant to only be used once for tasks deemed particularly sensitive—while others are "persistent"—meant to be used again and again. Some of these virtual machines come set up as ready-to-use templates, while others require an elaborate process of customization. The user models her digital

14 Qubes has developed in parallel to other FLOSS projects such as Tails, Subgraph, and Whonix, which together consider themselves part of an emergent "secure desktop ecosystem" grappling with the persistent failings of commercially available computing infrastructure and aiming at developing a secure system instead of trying to intervene on top of pre-built architecture.

presence across these separate compartments to make her experience more resilient to surveillance.

These functions add up to what can be understood as a counter-imaginary of compartmentalization. Rather than trying to "patch every single known security bug" in commercial OSs (Rutkowska and Wojtczuk, 2010: 5), Qubes seeks to limit the damage of potential attacks by re-organizing the OS architecture, with the goal of "not preventing exploitation but containing it, to minimize the problem" (Interview #2). It is important to note that compartmentalization is not "new" for human rights defenders or allied technical communities. In the case of one dedicated Qubes user, the optimization of isolation across various domains of life (e.g. work, personal, activism…) resonates with her decade-long activist experience: increased crackdowns and beatings of activists in her country spurred her to develop separate personal and professional identities as a safety strategy. Over time, she found that it became "natural" among her social groups to go by nicknames in "real life," "so you could do a Google search of each and they wouldn't be mixed" (Interview #40).
But how does the counter-imaginary of compartmentalization oppose the dominant imaginary of unavoidable surveillance? We hone in on the following two elements: domain isolation and anticipation. The first, borrowed from computer security and engineering, encourages users to envision their life as a series of distinct, separate "cubes," linking up the technical idea of digital isolation with the above Qubes user's analog strategy of identity management. A civil society technology manual called "Zen and the art of making technology work for you" (Tactical Tech Collective, 2015) reads,

> There are various approaches to digital security, but one of the most realistic approaches is security by isolation, which assumes that all security measures have their holes and therefore focuses on harm reduction by preventing possible

attackers from accessing the “whole system” that needs to be secured.

Qubes developers in fact argue that the field of computer security has long suffered from a persistent problem with digital domain isolation. A lack of effective isolation means that if one part of a machine is compromised, the rest can easily follow. In recent years, the computer security community has addressed issues around domain isolation with workarounds such as “virtual machines” and other contained computing environments, which aim to provide an extra “wall” between everyday computing experiences and unpredictable threats. However, running a system full of virtual machines can be an inconvenient and challenging proposition, causing problems with computing speed and memory, and requiring users to adapt to a new “flow” that is “not part of your body” (Interview #11). Here Qubes intervenes, offering a system built from the bottom-up to optimize for compartmentalization, while allowing its users to shape its particularities.

This control afforded to users, however, creates its own demands. Qubes comes with no default setting that would take care of every potential risk or even guide the user toward the most effective way of dealing with particular hazards. The second element of the compartmentalization imaginary is thus anticipation. In order to make effective use of the secure pockets offered by Qubes, users must on their own anticipate how their data might be compromised by adversaries. In other words, they must effectively “reverse engineer” how their digital traces might be used against them and disassemble their daily life into fragmented information flows to create effective, separate “security domains.” They must subsequently reassemble their daily workflow in a way that maps compartments to anticipated threats. As one user explained, in order to set himself up with Qubes, he had spent considerable time beforehand brainstorming how to separate his data and “fit” his life experience into the OS set-up. Yet, “once I had installed Qubes, I had trouble actually using it. It was unclear how you would actually put data in it and use it in a practical sense" (Interview #27).

"Partitioning one's digital life into security domains is certainly not an easy process and requires some thinking," cautions Rutkowska (2011). "This process is also very user-specific," she adds, acknowledging that what she has chosen to do might not align with the goals of others. In order to make the process of partitioning easier, Qubes held a workshop at a digital rights event, targeting a mix of digital security experts and human rights defenders. In this observed meeting, a Qubes volunteer demonstrated how she had gone about dividing her life into various subdomains, presenting a flow chart with four constructed "identities" classified as "public," "persistent," "pseudonymous," and "professional," with each mapping to a separate security domain. The volunteer then asked participants to create their own chart, identifying elements in their "digital lives" which "have a shared identity, have assets to protect, and denote high risk activities." Participants, armed with paper and markers, took to the task of re-imagining their personhoods as a series of discreet data flows. They described the freeing and "greedy" feeling of wanting to create more and more "safe," separate spaces for daily tasks and sensitive data. Yet, it was seen by some as a struggle to conceptualize how to effectively separate themselves into pieces—to understand which of the complex data flows of banal digital life do not in fact intersect?

The Qubes project constitutes a small-scale response to some of the particular problems of digital surveillance. The project tries to empower users to autonomously manage their digital life. By wiring isolated "safe spaces" into the mundane domain of networked computing, compartmentalization counteracts the dominant imaginary of presumed and unavoidable digital surveillance, "taming" its potentially destructive force. However, like other tools of its kind, the autonomy and safety it offers to users is tenuous and demanding of significant labor. The need for a user to engage in a sort of custom process of "dividuation" (Deleuze,

1992) and to successfully double-guess potential threats, puts the onus of responsibility for security on individual agency, a recurrent issue across technological interventions to surveillance harms (Kazansky, 2015). In addition, Qubes is limited in its ability to tackle the many issues adjacent to its immediate concerns with digital security, such as commercial privacy infringement, data exploitation, and algorithmic sorting. Interviewed Qubes users often tried to extend the affordances of Qubes into a tool to minimize data traces from online activities. This entailed the use of separate virtual machines for online shopping and social media in order to keep personal identities separate and thus frustrate commercial profiling. However, the users interviewed found it practically impossible to achieve this goal due to the many restrictions to anonymity imposed by commercial online platforms. Thus, while she feels digital security is practically possible, one of our Qubes users declared a sense of resignation vis-à-vis issues of privacy and tracking, lamenting that "the fight for privacy is a fight against windmills" (Interview #40). Our analysis shows that Qubes is a "stabilized" response offering security in the face of pervasive digital surveillance. Yet, its inability to grapple with the menace of corporate data practices highlights the limitations of the project—and explains the pressure for civil society to continue evolving its tactics of response to technological harms. With the continuous shift in corporate data practices and infrastructures, Qubes users and the larger milieu of civil society actors concerned with data exploitation find reason to seek out new interventions, one of which we next explore.

Dowse: counter-infrastructuring the datafied consumer

With the diffusion of IoT technologies and particularly "smart home" applications, people increasingly lose control of their network environment. Contrary to the physical milieu where one can easily realize when someone breaks in, intrusions in a digital network are difficult to detect. “There is no switch off button” to prevent something from going wrong with IoT devices (Interview #179). Developed as a community effort by the Amsterdam-based non-profit free software foundry Dyne (dyne.org), Dowse (dowse.eu) provides an intervention into the problems of IoT with open-source software that aims to “make it possible to connect objects and people in a friendly, conscious and responsible manner.”[15] Dowse software can be installed into an inexpensive microcomputer like the Raspberry Pi. Once operational, the “small box […] becomes the digital equivalent of a door and a curtain” (Dowse, n.d.), allowing users to modulate the access IoT devices have into the intimate space of the home.

The dominant imaginary Dowse seeks to consciously contrast is one of a pervasive, interconnected infrastructure controlled by centralized commercial players. The Dowse developers observe that commercial IoT infrastructures invoke a “magical” lifeworld of objects able to anticipate user needs (e.g. the fridge replacing the milk). What is left out of this “master narrative” (Interview #180) of IoT is the continuous data monitoring required for its “magic” to materialize. Thus, while this dominant imaginary promises to put user needs at the center, it also downplays its risks (cf. Lopez-Neira et al., 2019). In response, Dowse offers a curious twist on the notion of magic: rather than the obscuring “magic” of seamless technological utility, the Dowse developers invoke the language of magic to encourage users to get involved in a playful manner, with the goal of “open[ing] up the black box, dig deeper, look in the processes” (Interview #179). The “real objective is to convince people to dig” (Interview #180)—in other words, to proactively look for solutions against privacy infringement and data leakage.

15 See: https://www.dyne.org/software/dowse/.

This objective plays out in Dowse training and hacking workshops, which last 1 or 2 days and are designed to encourage attendees to "explore their environment with different eyes" (Interview #180) and to get their hands dirty with device set-up. The trainer—self-named the "Chief Magic Officer"—uses imaginative metaphors to engage people in a playful yet proactive manner (e.g. "witchcraft," the diviner's stick). He encourages attendees to "do magic" themselves, as opposed to merely suffering its consequences. It is a "narrative based on curiosity and manipulation, more than fights and opposition" (Interview #180). The "proactive digging" that Dowse designers aim to foster is enabled through "human-centric" software features designed to make the abstract threats of data exploitation concrete by "visualizing the invisible" (Interview #180). A flashing red button and a loud noise alert Dowse users of unusual or unwanted activity in their home network, detecting the presence of intrusive entities such as malware or spyware. With this function, the Dowse developers aim to "sanitize your data traffic" (Interview #180). The Dowse software further provides an interactive data visualization tool in order to make it easy for its users to recognize and name all of the digital applications active within their local network.

Working as "your IoT awareness device," Dowse creates a new mode of monitoring data exploitation in real time—which aims to reinstate user agency at the core of the network environment. The counter-imaginary of Dowse is thus centered around awareness. Building on sensory elements familiar to people (such as flashing lights and noise), it intends to offer a "collective path to consciousness" (Interview #179) in the era of IoT. By encouraging users to be alert, Dowse, however, potentially replicates "disempowering" logics, contributing to what Harvey et al. (2012) characterize as a "hyper-vigilant subject." This is where a professed focus on collective self-care comes into play. While Dowse risks augmenting the potentially paralyzing sense of individual responsibility for one's own security already discussed in relation to Qubes, the device incorporates symbolically and practically the notion of self-protection as a community effort, creating publics as mutual-care collectivities. As a developer explained, “We are not talking about you as an endangered individual. We are envisioning social situations in which problems can be addressed together” (Interview #179). It is worth noting that this emphasis on the collective dimension might also be a consequence of the fact that the project has roots in the open-source and hacker community. The “business” proposition from the beginning was to trigger a “response that becomes social” (Interview #180), by making Dowse boxes costing some USD 40-50 with a red led light. If it becomes red and flashing, you can switch off the button and call me, and say “hey, there is something wrong with the network.” (fieldwork notes)

The focus of the project on the “empowerment of yourself and your community” (Interview #179) also comes through in its technical language. Though its developers understand the project to be centered around issues of security, they try to reframe what security itself “means,” arguing that dominant discourses of digital and cyber security promote disempowering “superman thinking” and militarism (Interview #179). Dowse thus offers an intervention that is “not just a functional tool,” but also a symbolic operation proposing a different linguistic approach to networking. In conceptualizing and documenting Dowse, all references to military traits are removed: there is no use of “defense,” “shield,” “guardian” or “firewall” words. Privacy awareness (rather than protection) is envisioned and presented to its users not as a violent process, but as a responsible, natural act—one in search of harmony among those things connecting the inside and outside of a person’s private, common, and public aspects of life (Dyne.org Foundation, 2017: 3). The name of the project itself hides a symbolic intervention. Originally launched with the somewhat problematic name “Ghetto Box Do-It-Yourself,” its lead developer first targeted the tool at the hacker community. Later, however, the project was rebranded with the goal of “substituting the language” (Interview #180) to foreground the active role of individuals, including non-experts, in watching over their digital experience. As the creators explained,

> We want peace of mind, not paranoia […] Organiz[ing] this space [of IoT] to be hospitable but in control […] starts from language and representation. You cannot have a different network experience if you cannot imagine a networking situation which is peaceful […] We asked, "can we imagine an act of networking that doesn't imply firewalls, guardians, watchdogs, shields, threats?" We started talking about dowsing with a rod, with a magic stick, looking for the route. (Interview #179)

With its symbolic and technical interventions against pervasive data monitoring, the Dowse project presents a substantive response to the problems of commercial IoT. However, its propositions are somewhat fragile. Though Dowse is presented as a simple Do-It-Yourself hack, the technical set-up, as with Qubes, currently requires a certain labor of its users. As of writing, the take up of the project has been slow, requiring significant community engagement to achieve the collective practice it envisions. Furthermore, the "arms race to complexity makes it difficult for the home-brew to catch up" (Interview #180). Thus Dowse, in its current form, counters only a subset of issues that arise with pervasive data exploitation in the home. However, its symbolic intervention has already inspired other larger scale solutions developed with citizen empowerment in mind.[16] We thus characterize Dowse as a "formative" response to the threats of datafication, offering a tentative yet concrete intervention into the ever-evolving threats of IoT.

16 For example http://tools.dcentproject.eu

Against facial recognition: “feeling out” a response to the AI hype

Our Qubes case study concluded with a discussion of the apparent limitations of the project and the imaginary of compartmentalization it enacts. Noting the weakness of grassroots security projects as currently conceived, one interviewed Qubes user observes that “I don’t think [privacy/data tracking] can be an overarching fight that is won unless we win capitalism” (Interview #40), pointing to what she sees as an inherent limitation of “tool-centric” tactics against a broader onslaught of surveillance. She adds, “If you want to really do something, I don’t think it’s developing tools. I think it’s organizing a fight in the streets.” “And while people are organizing in the streets, how should they cope with smart facial recognition?,” we ask her, probing the tension between tactical interventions and broader civil society strategies. Here she points to another sort of “tool,” admitting “I’m a fan of the makeup [experiments].”

The “makeup” she is referring to is a “look book” of bold face paint patterns designed by artist Adam Harvey to render human faces incomprehensible to roving facial recognition algorithms. Titled “CV Dazzle” (cvdazzle.com), the project focuses on countering Open CV, one particular algorithm used across different kinds of data infrastructures to power automated face surveillance. Released in 2010, the name CV Dazzle takes inspiration from the First World War practice of “Dazzle Painting” camouflage to thwart attacks against merchant ships by German U-boat captains (Murphy and Bellamy, 2009). In recent years, obfuscation and camouflage-related projects such as CV Dazzle have become a recurring locus of intervention within different kinds of projects aiming to resist data-driven surveillance (Monahan, 2015). Artists and activists have played with makeup tutorials (Mayer, 2013), organized “Facial Recognition Defense Workshops” (Lewis, 2013), and created spin-off applications (Face Dazzler, n.d.) indicative of what De Vries and Schinkel (2019) understand as a manifestation of "algorithmic anxiety" over the looming threats of ubiquitous face surveillance—which might portend a broader "anti-facial recognition movement" (Cox, 2014). Indeed, our fieldwork highlights that recent developments in AI and automation are perceived by civil society to be the most troubling, if also "overhyped" issues of current concern. One long-working digital security advocate interviewed was in the midst of transitioning his work from more "traditional" digital security concerns to explicitly AI-focused projects. Explaining this shift, he noted,

> We have to come up with a framework for understanding digital security in a context of AI taking over. I don't know what it's going to look like, but I think we all have to be much more imaginative and creative about what that future's going to look like and how we are going to exist in it. (Interview #43)

This interviewee's anxieties expose a tension between unknown data futures and the long-known harms already affecting particular communities and populations (Gangadharan and Niklas, 2018). From this tension, an imperative emerges among civil society actors to coalesce around a shared vision of social justice vis-à-vis AI. Here CV Dazzle offers a playful intervention to creatively imagine new responses to a shifting milieu of threats. Specifically, we see CV Dazzle as the encapsulation of an emerging counter-imaginary of obfuscation, aiming to protect the autonomy of the body and personhood through tactics which obscure or distort the data collected by states and corporations. CV Dazzle, we argue, is an example of a "speculative" response to datafication-related threats, in the sense that its focus is to "feel out" the contours of emerging issues, the stakes of which are as of now uncertain. It does so by endeavoring to raise awareness on an issue by making a complex and quickly moving problem "thinkable" and "senseable."

Our fieldwork took us to a 2-hour workshop leading a group of transnational civil society actors through the contours of CV Dazzle, exploring its possibilities as a form of self-defense. In the midst of a large conference on topics of digital rights and Internet freedom, a "facilitator" stood at the front of a room of attendees, offering a provocation: "I am going to try to make the algorithms think this is not a mouth," she told us, drawing a large black smudge diagonally across her lips. She then positioned herself in front of her laptop to see if the camera, running facial recognition algorithms, would register her face as a face. Members of the audience went on to volunteer to be covered in face paint according to the methodologies of CV Dazzle. The facilitator drew a bold black streak in one direction. Then another. The facial recognition software she had open on her laptop continued to register the various computational "frames" that make up her face, which the audience could deduce by noticing that the face continued to appear "in focus." As the facilitator grew increasingly desperate to thwart the algorithm, her face paint patterns transmogrified into new and unexpected shapes, eliciting laughter from the audience. Success finally came when the facilitator blocked over half of the volunteer's face with a thick cover of hair, the room erupting in cheers. The facilitator explained that the obfuscation enabled by CV dazzle "means that instead of not giving information to the algorithm, you throw information towards the algorithm," a self-defensive practice highlighted by many civil society actors we interviewed as inevitable in an environment in which refusal to comply with requests for biometric data is increasingly difficult. What, then, does CV Dazzle indicate about the directions of civil society responses to the looming threats of algorithms, machine learning, and AI?

As we write, a number of pathways are signaled. For example, grassroots actors and academics increasingly argue that solutionist approaches to "fix" AI, as with recent efforts to ensure "fairness" in algorithmic decision-making, are disingenuous attempts to narrow a broader justice agenda, allowing the industry to delimit the "problems" of AI in ways that elude substantive accountability (Hoffmann, 2019). Civil society should instead ask the fundamental question as to whether such a technology should exist in the first place, argue advocates Ahmed and Aoun (2018). In parallel, US community activists and academics push for an abolitionist agenda to counter emergent modes of data-driven oppression, responding to a historical continuum of harm to marginalized and dispossessed populations (Datafication and Community Activism Workshop, 2019). The right to refuse the deployment and diffusion of harmful technological developments are framed as a central point to push amid the corporate discourse on AI.

What then to make of the self-defensive counter surveillance tactics promoted by CV Dazzle? By making space for participants to play around in provocative manners, CV Dazzle might arguably promote what has been scorned as the “aestheticization (and individuation) of resistance” (Monahan, 2015). Yet, tactics playing with “individual avoidance” (Monahan, 2015: 162) arguably also promote critical technological engagement, building on a tradition of playful subversion for awareness-raising (e.g. Critical Arts Ensemble, 2001). In an interview with the facilitator of the workshop, she made pains to explain that the point of the experiment was not necessarily to propose that people “go out into the streets” wearing bright if dubious makeup, but to start “a conversation of how these technologies are being used and what can we do protect our bodies from becoming templates”—in other words, a mold to “fit in.” CV Dazzle itself disclaims any promise of universal utility; the project’s website includes a note in small text warning that “in the meantime, everything here is designed for the OpenCV haarcascade face detection algorithm” alluding to the ephemeral quality of tactical “effectiveness” in obfuscation techniques—something Brunton and Nissenbaum (2015) also acknowledge. Indeed, the utility of such a project is continuously threatened with obsolescence vis-à-vis the continuous optimization of algorithms and data infrastructures (Gürses et al., 2018). Ultimately, CV Dazzle and its speculative appropriation toward activist purposes signals the continued, if shifting tactical utility of "tools" amid broader struggles and mobilizations, which must be associated with "something at a social level," as our Qubes "user" notes (Interview # 40) and Dowse developers also point to.

Conclusion

This chapter has addressed the emergence of counter-imaginaries within the civil society commitment to oppose dominant imaginaries of datafication as constructed by state and corporate interests. Whereas dominant imaginaries of datafication configure users as either co-producers of surveillance or its helpless victims, the projects we highlight in this chapter try to bulwark autonomy, increase agency, and provoke critical inquiry into new ways of being and doing amid the threats of pervasive datafication. Our first case explored the counter-imaginary of compartmentalization as a pathway to harm reduction amid assumed surveillance, as inscribed within the Qubes OS. The second case looked at Dowse, a project aiming to create an off-switch "button" for people caught within the pervasive datafication of the IoT, identifying the counter-imaginary of awareness. Our third case examined CV Dazzle, which, by playing with a counter-imaginary of obfuscation, provides a way for civil society actors to "feel out" the threats of face surveillance.

With a sophisticated architecture, dedicated team and "core" group of volunteers and users, Qubes can be understood as a stabilized response to the threats of datafication. Despite various struggles, it actively strives to make itself practical for a wider community. As a formative response, Dowse provides an important new capability to its imagined users. Yet, as a "demo," it still seeks a broader community to mobilize its ideas of collective self-care. Though the actors involved with Qubes and Dowse have, to different degrees, solidified a repertoire of effective response to identified threats, they find themselves exposed to an onslaught of commercial data exploitation that overflows the bounds of their respective projects. Meanwhile, those who play with CV Dazzle for speculative purposes absolve the project of practical utility: CV Dazzle makes no attempt to comprehensively counter the threat in question, sticking explicitly to the limited timescales of tactical effectiveness.

As small, scarcely funded projects, Qubes, Dowse, and CV Dazzle together mount a tenuous struggle against the powerful interests and infrastructures that produce a shifting landscape of threats. This shifting landscape necessitates a continued re-imagination of effective tactical interventions. Yet, in their small interventions, the projects we highlight build out values, ideas, and symbols which try to re-imagine life amid datafication, and to variably reclaim that people (and their bodies) are more than just templates for surveillance (fieldwork notes). We note that as counter-imaginaries, compartmentalization, awareness, and obfuscation are not merely utopic, serving instead to expose civil society's ambiguous relationship to notions of individual responsibility. As configured in the three projects, these counter-imaginaries cast individual users as the locus of agency, requiring them to grapple with high technological complexity in the name of protection from the harms of datafication. Yet, this protection is not seen by civil society actors to be forthcoming from other sources, giving their attempts an outsize significance. We argue that the role of these technical interventions should thus be contextualized within broader civil society strategies. What warrants further investigation is the role such projects play in the construction of a larger "contentious politics of data" (Beraldo and Milan, 2019) which interrogates "the ways in which data has become such an object of power" and explores "how to critically intervene" (Ruppert et al., 2017).

Chapter 6. Taming uncertainty into risk: Towards a critical lens on risk management practices in digital and cybersecurity[17]

17 This chapter has been submitted for peer review in July, 2021

Abstract

Amidst myriad forms of contemporary governmental and commercial digital surveillance, civil society actors grapple with a number of threats and uncertainties related to digital intrusions, online profiling, harassment, and technology-facilitated violence. This chapter explores how targeted civil society actors work with digital security specialists work to tame surveillance-related uncertainties into 'manageable' risks. The chapter investigates risk assessment as it is enacted in the context of a digital security training organized for human rights defenders to learn concrete security mitigations such as encrypted communications tools. Drawing on ethnographic data from participant observation in 12 digital security trainings organized for human rights defenders, the chapter shows that in the context of the digital security training, the transformation of uncertainty into risk occurs through the development of a shared language about danger. I term this process one of 'qualculative convergence', a critical intervention into corporate risk management language which conceives of risk as a cold and quantifiable phenomena. The chapter draws on valuation studies and studies of risk calculation in STS to enrich an interdisciplinary understanding of how people make sense of uncertainty. In exploring how targeted communities apply risk-centric logics to their work, the chapter also extends critical security studies' long-standing concerns with the ethico-political dimensions of risk beyond its focus on state and corporate security actors.

Keywords: risk assessment, risk management, risk calculation, qualculation, valuation studies, digital security, cybersecurity

Introduction

The rationalities and techniques of risk management are of central interest to studies of security, surveillance, and algorithmic, data-driven profiling (c.f. Amoore, 2013; Amoore and de Goede, 2008; de Goede, 2004; 2008; Dencik et al., 2019; Gandy, 2009; Monahan, 2010; Stachowitsch and Sachseder, 2019). Who or what is framed by institutions as risky or at risk serves to justify the development and deployment of novel forms of surveillance against different populations, entrenching inequalities and enrolling people within 'anticipatory regimes'(c.f. Adams et al., 2009) of disciplinary power. As Amoore (2013) and O'Grady (2016) argue, risk logics and practices are highly mobile, traveling across disparate social realms to inform rationalities around security, safety and emergency response. Yet the focus of much critical risk and security literature has historically been the logics of state and corporate risk regimes. This chapter instead explores the risk-centric practices of civil society actors seeking to resist and find safety from the harms of digital surveillance and 'digital threats' related to online harassment, data theft, and intrusion into digital infrastructures. The chapter investigates how surveillance and security risks are made sense of by civil society actors in the context of digital security trainings, events organized to facilitate learning about mitigation strategies against common forms of digital attacks and compromise caused by state and corporate actors antagonistic to civil society goals.

The threats and uncertainties of concern to civil society actors attending digital security trainings cover a range of different issues related to surveillance, security, and datafication; from concern over the spread of wide-scale 'smart' facial recognition infrastructures to the individual targeting of high-profile HRDs through sophisticated state-sponsored malware. The continued uncertainty over how exactly surveillance is conducted and whether an individual or group are being targeted at any given moment contributes to a sense of overwhelm for those seeking safety, as I show in Chapter 4 of the thesis. Civil society groups therefore work to grapple with these uncertainties in a way that facilitates agency and safety. As Chapter 5 shows, this can mean turning to different forms of technological mitigations and risk management strategies to 'tame' uncertainty. Yet, per Scoones and Sterling (2020), 'uncertainty is never just a technical issue'(15). Scoones and Sterling argue that 'addressing uncertainty means confronting inequality, vulnerability, precarity and the deeply embedded inheritances of history head-on'. The authors further suggest that turning to risk management to deal with violence and danger rarely results in doing away with the risk of concern. Rather, it provides violence and danger with an aura of manageability. What does this mean for the efforts of civil society actors who apply different tools and techniques of risk management to deal with digital surveillance and insecurity? Taking inspiration from Scoones and Stirling, this chapter looks closely and critically at how dangers related to surveillance and digital insecurity are flattened into manageable contingencies and mapped to appropriate mitigations for anticipated threats through techniques of risk management. Further, the chapter proposes a critical intervention into risk management approaches through a concept aiming to de-naturalize the corporate rationalities that inform the risk-centric practices of civil society and other social realms.

Importantly, the uncertainties of concern to civil society actors result from political instability, shifting patterns of discrimination and targeting, and ubiquitous yet opaque data processing, with well documented yet difficult to avoid harms. In the face of such ubiquitous and power-laden dynamics, the setting of the digital security training becomes a place to come up with concrete actions that can be taken on an individual and community level in order to continue human rights and social justice related work with some degree of autonomy and safety. While in Chapter 4, I traced the growing importance of civil society practices configured to grapple with and 'tame' the uncertainties that surround contemporary surveillance and its related threats. In this chapter, I analyse the enactment of a risk assessment process at the site of a digital security training organized for human rights defenders to learn mitigations to digital surveillance and security threats from state actors antagonistic towards their political goals. Within the realm of civil society[18], digital security training events are set up as a space to 'raise awareness' of threatening technological and political developments, build literacy around the stakes of data and the digital, and develop concrete counter-strategies against ever-proliferating forms of surveillance (Daskal, 2018; Ermoshina and Musiani, 2018; Kazansky, 2015, 2016; Monsees, 2020; the Engine Room 2018). Training participants – which in this chapter are human rights defenders working on a diverse range of issues such as environmental justice, anti-corruption, and women's rights – are asked to share personal experiences with surveillance, work hands-on with digital security tools such as secure browsers and messenger apps, and coalesce around potential strategies for action in response to past or probable harm.

Digital security trainings are varied in their scope and shape. Though 'digital security' is the stated subject, the term encompasses a wide range of technology related topics including secure data storage, 'information management', communications, and censorship circumvention, as well as issues around 'data politics'(Ruppert et al., 2017), autonomy, 'technological sovereignty' (Couture and Toupin 2019; Haché, 2014; 2018), algorithms, and digital rights (Daskal, 2018). The focus is on turning unwieldy technological complexity and political uncertainty into a manageable risk, as I show in Chapter 4. But what goes into this transformation? How does it become possible for groups under threat to

18 Civil society in this chapter refers to the ream of action beyond the state and corporation. Of particular focus is an institutional ecology of transnationally coordinating non-profit organizations, security specialists, and front-line groups, which together grapple with the threats of digital surveillance and related harms around harassment, targeting, and discrimination.

think through ‘data mess’? (c.f. Pink et al., 2018). More fundamentally, why is it important for some to imagine political strife and injustice through the language of risk, and how might thinking through the language of risk change the nature of civil society work?

In this chapter, I show that in the context of the digital security training, the transformation of uncertainty into risk occurs through the work of what one digital security trainer describes as the development of a ‘shared language’ about danger, through which ‘the individual can act’ (Interview #12) in anticipatory avoidance of undesired future events. I term this process of developing a shared risk language as a process of ‘qualculative convergence’. As I will expand upon further in the next sections, the concept of qualculative convergence is a critical intervention into the concept of ‘risk convergence’, a term that is increasingly popular in corporate enterprise risk management, which means, ‘to integrate risk disciplines that are significant to an organization, such as operational risk or compliance, within a single framework’ (Enterprise Risk Management Initiative, 2008). Where risk convergence is premised on a ‘rational’, financialized, and quantitative approach to risk, my concept of qualculative convergence pushes back against such risk rationalities. I make this intervention by drawing on the notion of ‘qualculation’ (Callon and Law, 2005; Cochoy 2008), a concept which explains human judgement as the product of messy, intersubjective forms of valuation. As Callon, Law, and Cochoy argue, when people evaluate, calculate, measure, and otherwise engage in different processes of judgement, the lines between quantitative and qualitative thinking are in fact blurry. In other words, even a quantitative judgement involves complex processes of estimation, visual guessing, and other forms of incommensurable knowledge. The interwovenness of quantitative and qualitative judgement means that hard distinctions between the two occlude a granular understanding of the complex social processes that produce numbers, heuristics, standards of measurement, and infrastructures. These three authors hence suggest the use of the term 'qualculation' in order to draw attention to the messiness of human judgement.

I apply Callon, Law, and Cochoy's concept of qualculation within my own concept of qualculative convergence in order to build an understanding how human rights defenders and digital security trainers make sense of surveillance uncertainties. The chapter explores how the process of qualculative convergence brings people together around a shared notion of security risk. In exploring qualculative convergence, I attend to the affective, temporal, and material elements of this process. In exploring how uncertainty becomes risk through qualculative means, I aim to contribute to a richer understanding of how people make sense of datafication through different forms of calculative (or rather, qualculative) logics. Furthermore, in exploring how civil society actors such as human rights defenders apply risk-centric logics to their work, my aim is to take the long-standing field of study in critical security studies around risk beyond its focus on state and corporate security actors. As I argue, attending to civil society practice can enable critical security studies and other disciplines critically concerned with risk to build a richer empirical understanding of the mobility of risk practices and risk logics, illuminating paths through which risk rationalities and security practices are not just imported into new sociopolitical contexts but also reconfigured and reimagined.

The plan of the chapter is such: I first situate my concern with risk in the context of critical studies of security and explain my conceptual intervention into cybersecurity risk management. Following, I explain my methods. I then describe three stages of ‘qualculative convergence’ in the context of a digital security training, drawing on data collected from three years of participant observation in digital security trainings.

Questioning Risk

Cybersecurity historian Rebecca Slayton has argued that 'risk management is the central approach to cybersecurity in governments and corporations around the world' (2015: 32). Risk assessment in this realm is increasingly a highly formalized process, premised on convergence around a set of 'objective' quantitative metrics. Slayton investigates how risk management strategies provide cybersecurity entities and institutions with a sense of control – its penultimate embodiment in the appeal of automation and automated risk models, through which 'analysts could 'turn the crank' to output a measure of risk, without really understanding what they were doing' (33). My own survey of cybersecurity and information security literature since the 1980s highlights that computer science departments, commercial and state cybersecurity institutions predominantly draw on rationalist and cognitive approaches to risk in support of 'objective' frameworks for risk management. A number of studies focus on the psychological and behavioural-economic aspects of 'risk perception', postulating on why degrees of risk perception vary amongst individuals and groups (Acquisti, 2007; 2010; Asgharpour et al., 2007; Blythe and Camp, 2012; Wash and Rader, 2011). What is largely missing from this literature is a critical perspective on how experiences of surveillance and digital danger, threat, and harm become thinkable as 'risk' in the first place. Instead, risk is cast as a self-evident 'natural' phenomena dealt with in either 'rational' or 'irrational' ways. The result is an emphasis on why people fail to perceive risk – or how to better quantify it.

Drawing on the work of cultural anthropologist Mary Douglas (1992), I argue that this ignores the institutions that are responsible for danger and its harms in the first place, instead placing the onus on the individual's behaviours as a moral failing (c.f. Barnard-Wills, 2012; Kazansky, 2015; 2016). In order to break beyond this limited understanding of risk, it is useful to follow the line of scholars studying risks and threats not as givens but as the constructive result of a process of grappling with uncertainty (c.f. Amoore, 2013; Amoore and de Goede, 2008; de Goede, 2004; 2008). Scholars critically studying the logics and rationalities of risk have long observed how the concept of risk shapes the way we think about the world. As these critical scholars observe, risk is danger or uncertainty made manageable or exploitable. Examining how uncertain, dangerous, and harmful situations are cast by risk-centric framings as manageable risks and exploitable opportunities, Douglas points to its 'universalizing terminology, its abstractness its power of condensation, its scientificity, its connection with objective analysis' (15). Where sociologist of risk Ulrich Beck's concerns lie with the proliferation of globalized risks (1992), Douglas explores how the ubiquitous 'language of risk' serves to spread and shape our thinking about danger through its narrow lens (14), urging scholars to attend to the culturally specific ways that risk is framed by powerful institutions. In more contemporary literature, scholars have taken this call forward through work examining the construction of risk and management of threats within algorithmic surveillance processes; literatures on the audit society (Gandy, 2009; Power, 2007) in the critique of the war on terror (Aradau and van Munster 2008; de Goede, Simon, and Hoijtink 2014; Suchman, 2019); predictive policing (Andrejevic,2017; Massumi, 2015) and risk scoring (Dencik et al., 2019).

These scholars look at how security 'threats are rendered perceptible through algorithmic calculative devices, logics and techniques' (Dencik et al., 2018:1435) and how risk analysis serves as a 'sense-making security practice '(Stachowitsch and Sachseder, 2019: 108). The critical study of risk management, however, remains under-developed in relation to contemporary cybersecurity in state and corporate realms, with the exception of work by scholars such as Slayton (2015; 2020) and Ermoshina and Musiani (2017; 2018) in relation to practices particular to civil society. Slayton's historical work on state and corporate cybersecurity is particularly relevant for clues on how to study this area of practice as it pertains to my study of risk management within a civil society digital security training. In exploring the history of state and corporate cybersecurity, Slayton shows that despite its scientized aura of objectivity, risk management is processual and highly contingent on the messiness of qualitative human judgement (2015). Through an intensified focus on structured, automated, and quantitative metrics, she argues that risk management provides a false sense of control which obscures 'the most valuable part of risk assessment….namely, the learning that came from the process of measuring risk rather than the final measurement' (33). This process of arriving at risk (and the intersubjective learning therein) is what my chapter is primarily concerned with. However, rather than conceiving of risk measurement as either strictly qualitative or quantitative, it explores the messy, oft un-quantifiable processes of valuation which nonetheless draw on the language of probabilistic risk to tame uncertainty. While the above work has focused on state and corporate regimes of threat construction and risk management, this chapter brings these questions to the context of civil society work, looking at how risk emerges as the product of a sociomaterial process of sensemaking concerned with the anticipation of harm.

Qualculative Convergence

This chapter traces how the uncertainties of surveillance are made into a manageable problem through the collective production of a risk heuristic within a digital security training. In this section of the chapter, I explain my inspiration for developing the concept of qualculative convergence as a way to describe this process. As I argue in Chapters 4 and 5, security and risk practices and their logics have a way of 'traveling' across social realms (c.f. Amoore, 2013; O'Grady, 2016), making their way into the practices of actors upholding values beyond the state and corporation. Risk assessment is one such mobile practice, which I focus on exploring here. While in Chapter 4, I investigated risk assessment through thin description of its mobility across different civil society contexts, in this chapter, I look at how particular assumptions of risk assessment are both appropriated and flipped on its head in the context of a civil society digital security training. I myself make a critical intervention into risk management tropes through the development of a particular concept to describe the process of how risk is tamed in a digital security training – which I call qualculative convergence. In developing the concept of qualculative convergence, I found particular inspiration from a security-focused technologist who I interviewed during my fieldwork. This technologist was charged with building an institutional risk management approach for a large human rights and development organization in the world in order to better contend with the prevalence of 'digital threats' against civil society organizations around the world (Maschmeyer et al., 2020; the Citizen Lab, 2014). Discussing the search for an appropriate institutional risk management approach, the technologist expressed frustration with existing methodologies for addressing digital security risk, explaining that the technical approaches from computer science which he had explored failed to account for the 'human' and institutional dimensions of security. Furthermore, risk focused on the individual rather than group-level concerns.

In our interview, the security specialist told me that in his research, the most useful approach he had come across for understanding risk beyond the 'individual level' came from the corporate-centric realm of enterprise risk management. Enterprise risk management is a field of practice concerned with unifying risk centric thought and action within institutional and organizational contexts (Power, 2007; 2009). Enterprise risk management literature casts the unification of risk management approaches as a central goal of contemporary corporate management cultures. A unified approach to risks (and hence its correlate of opportunities) is seen to bring greater efficiency to organizational processes, and hence, better corporate profit bottom lines. It was in exploring literature on enterprise risk management that I came across the concept of ‘risk convergence’. Risk convergence is a concept describing a multi-pronged managerially-driven effort to unify approaches to risk management across an organization. The process involves identifying and bringing together disparate risk frameworks under one unified approach (Enterprise Risk Management Initiative, 2008). Risk convergence would seem to exist in a separate realm from the civil society practices I study, but in fact, my interviews with digital security specialists at large NGOs indicate that enterprise risk management is an appealing framework for organizing thinking about dangers and hazards, because it offers a way to unify disparate concerns around security and safety – whether financial, physical, or digital. The appeal of being able to integrate or converge these various concerns speaks to the fact that nonprofit organizations are also guided and constrained by financial bottom lines. While the details of these financial aspects remain out of scope of this chapter, the important point here is that viewing danger and security through the lens of efficiency and asset management makes sense beyond the corporate realm, something I also document in Chapter 4.

For the purposes of conceptualising risk within a digital security training and developing my concept of qualculative convergence, I find risk convergence a useful term for both what it does and does not do. What the concept does is to give a name to the difficult process of arriving at a uniform lens on risk. What it does not do is challenge the corporate rationalities of risk. This chapter sees the notion of risk convergence as an instrument for dealing with uncertainty which is bound primarily to profit, and through which security threats are primarily equivocated with threats to the function of business. Exemplifying an entrenched model of corporate risk management, it is troubling for the way it conceives of and constructs risk, focusing as it does on how unwanted intruders (from both without and within) affect financial bottom lines (c.f. Power, 2007; 2009).

In doing so, this conception of risk management does not seem to match the expressed values and politics of the human rights defenders and the civil society digital security practices which are the focus of this study.

This chapter does not posit that it is possible to reform corporate approaches to risk management. As Douglas would argue, the problem of 'risk' begins elsewhere. In other words, the way risk is constructed is an artefact of an institution's values as well as its valuation practices. Rather than trying to reform corporatist approaches to risk, I make a small subversion to the concept of risk convergence in order to use it for the purposes of my analysis in this chapter. I use the concept as s a starting point from which to investigate the ambivalence of risk management as it is enacted in a rather different context than corporate security. My subversion into the concept is to flip its rationalist underpinnings. As Stachowitsch and Sachseder (2019) put it, 'risk analysis – like any form of knowledge production – is not a neutral and objective assessment of a reality outside of itself, but co-constitutive of its own subject' (108). Rather than assume the pre-existence of risk as an objective phenomena which only requires capture and convergence into a single framework, I show that it is not risk that is converged, but the imaginaries, anxieties, and experiences of danger shared by people brought together into discussion about danger. This convergence of human experience occurs through a process that entails valuating the messes of data, uncertainties of surveillance, and hazards of life within a shared space. In the context of risk assessment, convergence culminates in the flattening of human experience with uncertainty into a single, structured risk heuristic.

Instead of holding to the term 'risk convergence' to describe the flattening of unwieldy uncertainty into a unified understanding of risk, I describe the process as one of 'qualculative convergence'. Though a mouthful, the term provides an alternate way to think about how uncertainty is becomes understood through the calculative language of risk. In developing this concept, I draw on the concept of qualculation, as developed by Callon and Law (2005) and Cochoy (2008). These three sociologists of knowledge characterize calculation as sociomaterial process of valuation bounded by time and space. Callon and Law work from the assumption that calculation, rather than a strictly mathematical or 'quantitative' process, is entangled with or even indistinct from different forms of qualitative judgement and valuation. Nor, they argue, do calculative processes necessarily lead to any sort of numerical output. In summary, their important move is to advance interdisciplinary understandings of of calculative rationalities by collapsing the 'distinction between the quantitative and the qualitative' (Callon and Law, 2005: 719). They emphasize that calculation 'often has nothing to do with quantification'(730), and instead argue that it is better understood as 'a process in which entities are detached from other contexts, reworked, displayed, related, manipulated, transformed, and summed in a single space' (730). What ends as a neat output in the form of a number – or not – begins as people, ideas, and assorted material elements, which through a process of valuation is flattened onto a single plane. From this: 'a result is extracted. A new entity is produced. A ranking, a sum, a decision. A judgment. A calculation' (719). In the following sections, I draw further on Callon, Law, and Cochoy's understanding of *calculation as human mess* in order to generate a critical distance from rationalist discourses of risk.

Methods

This chapter draws on data collected through ethnographic fieldwork and interviews from 2016-2019 of digital security trainings and awareness-raising events. I conducted participant observation a total of 12 workshops and trainings taking place in Europe and Southeast Asia. Specific locations and names of participants and their organizations are anonymized in line with a research ethics protocol developed by myself together with input from the research participants. This protocol emphasized the anonymization of interviewees, the de-identification of particular events, people, and places, and a set of stringent, context-specific data security measures including encrypted data storage and communications. Some events attended were open to anyone interested in attending from within the larger civil society conferences where they took place, while two were by invitation only due to safety concerns. In addition to shorter 'open' workshops, I attended two multi-day, closed digital security trainings in 2017, each spanning five days in length. The focus of description in this chapter is on my observation of one of these events, which was geared towards addressing the particular experiences of human rights defenders and activists believed to be actively 'under threat' from state or commercial actors conducting surveillance or any number of other sources of potential harm. The training, for reasons of safety, took place away from the public, with special attention put into creating a temporary space removed from fear and trauma that accompany targeting and surveillance. Intended for people working at the 'front lines' of social movements engaged in rights-based work, attendees were brought temporarily out of urgent work environments, where they were held in suspense for a temporary period of recovery and strategy building.

The training I observed was a 'general' introductory security training for rights defenders considered 'at risk' of targeted attacks for their work. Though the training took place in Europe, it brought together participants from all over the world, many of whom had left urgent circumstances in their work to counter issues such as violence against women, indigenous land grabbing, and environmental destruction. It covered topics of information management, censorship circumvention, secure data storage, secure communication, and data politics. In addition to participant observation, I conducted semi-structured interviews with several participants as well as the trainer as time would become available during the event. In interviews, I asked the trainer featured in this chapter – as well as in the other events I attended – how they identified threats and how they talked about risks and threats with participants. I asked participants to reflect on their motivation to attend the training and how they did (or did not) find it useful to their work. A note on issues of research access relating to my participation observation: my participation at the closed trainings I attended for my research followed only after an assessment, 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 back an analysis of my observations to the organizers directly following my attendance in order to gain a sense of research topics which might be a 'no-go' for safety reasons. Just as importantly, this provided the research an action-oriented outcome by immediately providing back information that might be directly useful to the group.

Steps towards qualculative convergence

This section of the chapter breaks down qualculative convergence into several processual stages taking place over the course of a digital security training. I note that I have identified these stages through inductive analysis of interviews and participant observation in 12 total workshops and trainings related to digital security. I then brought my analysis back to the particular site of the digital security training featured in this chapter. In conceptualising these stages of qualculative convergence, I found inspiration from the three-stage process of calculation put forth by Callon and Law (2005). In the **first stage** of qualitative convergence, which I call 'creating the space', the digital security trainer and human rights defenders work to establish agreements and expectations for what will happen in the training space. They also begin to discuss how they define important definitions related to security, risk, and technological threats. In the

second stage of qualculative convergence, which I call 'enumerating uncertainties', human rights defenders share – or enumerate-- stories about their experiences with surveillance. The trainer works to find threads in these stories, weaving them together to find common concerns. Finally, in the **third stage** of qualculative convergence, – which I call ‘commensurating problems and solutions’ – the digital security trainer brings these stories and concerns together – or, commensurates them – through a risk analysis which focuses on the situations surfaced by the human rights.

The ‘product’ (per the language used by Callon and Law, 2005) of this process is an intersubjective notion of risk taking the form of a risk heuristic. This risk heuristic therefore establishes a ‘shared language’ (Interview #12) around risk. The risk heuristic may take shape in the form of something as simple as a list on a piece of paper, a quantified, computable risk calculation, or in the grid of a visual ‘risk matrix’ (Jordan et al., 2016) – as I will describe in this chapter. This risk heuristic is then used help human rights defenders choose tools tactics and strategies, or so-called ‘solutions’. The aim is to come out of such a training with a repertoire of strategies and tactics to mitigate the harms of surveillance, so that ‘at the end of it [the training] the individual can act’ (Interview #12). Thus, in the third stage, the trainer and group together apply the agreed-upon risk heuristic to choose appropriate security mitigations and make plans for how to implement and integrate them in their daily lives beyond the training space. Beyond the training space, these ‘solutions’ must still be transitioned back out of the artificial boundary of the training space and into the daily practices of human rights defenders and NGOs. Perhaps the most crucial stage for civil society actors, this is also where the chapter ends – and where my previous work begins. The many challenges and contestations of integrating security practices remain out of the scope of this chapter, however I have explored this issue extensively in my previous research (Kazansky, 2016). In the next sections of this chapter, I go through each stage of qualculative convergence.

I: Creating the space

It is the first morning of the digital security training. A group of human rights defenders, all coming from different countries and regions of the world, is seated on the floor in a circle. Many have taken red-eye flights to arrive at a place deemed temporarily ‘safe enough’ to gather and openly discuss matters of security. The room is lit by a panel of fluorescent lights and lined in grey carpeting. The corporate décor of the room gives it a generic placelessness. This, the participants are told by the trainer, is a space that offers a chance to recover, reflect, and strategize. Its remoteness from the every day is intentional –as are the multiple exit doors in case of emergency. The training is a place where for the next five days, the participants will discuss and test practices for how to conduct human rights work amidst continued dangers and threats and how to act when everything is uncertain. To conduct such a training requires the creation of a particular kind of space, one that is physically, psychosocially, and ‘digitally’ secure, a number of interviewed trainers underline. One explains that as part of his job to create security strategies, ‘the first thing I have to do is to create a space for participants to be able to actually perceive or come up with their understanding of the situation at hand...‘away from the trauma that they’re in, or on the other hand, the flat affect that comes from trauma’ (Interview #7). Only in a space free from immediate dangers and concerns, can analysis of risks take place. As the trainer leading this training in particular explains, this ‘safe space’ ‘sets the stage’ for risk assessment (Interview #9). Further:

> It’s about creating and maintaining that kind of space where participants talk about ‘this is my situation and these are the things that are threatening my sustainability, and no one is going to judge me; say that it was my fault that I left my door unlocked, or my phone unlocked’, that’s my space (Interview #9).

To construct such a space, the trainer prepares for the training by investigating the grounds for signs of physical surveillance and compromised telecommunications infrastructure. Through investigation, the trainer learns that the Internet service provider bringing wifi into the space is known to hand data over to the local national security agency for monitoring. To counter this threat, the facilitator decides to supplant the provided telecommunications infrastructure with his own, providing Internet access through his personal mobile hotspot. All of these safety preparations are done before the participants have arrived to the space. With the arrival of the participants, the ‘facilitator’ positions himself at the edge of the circle, marking the beginning of the digital security training, which will last five days. Expectations are established to further delimit the space as a safe space. The facilitator lays out some ground rules: no photos are to be taken of anything in the room. Harassment in all forms is prohibited. It is jarring – perhaps inappropriate – to imagine that walking through the door of a room in some remote place could suddenly wipe clean the burdens of life under threat. Yet, the trainer’s practice of space-making holds resonance with notions of spaces as a conduit for free-thinking, safety, autonomy, and prefigurative politics (Boggs, 1977; Epstein, 1991; Polletta, 1999). For the interviewed trainer, the space to be created should particularly embody the values and priorities particular to civil society and ‘defending our space for work’ from those opposed to human rights, as described in the digital security training methodology manual titled ‘Holistic Security: A Strategy Guide’ (Tactical Technology Collective, 2016: 20). Not only do the authors of the manual speak of defending civil society’s ‘space’, but they also seek to expand it by pushing for the extension of human rights in hostile spaces. Creating this space within a training symbolizes the first step for defending and expanding civil society space out in the world.

Further activities are chosen to help ‘create the space’. Shared definitions around technological and security concepts must be stablished. ‘What does security actually mean to you?’ the facilitator asks the group, pointing a marker at a flip chart. One person calls out ‘the military’; another, ‘violence’; a third, ‘protection’. The facilitator puts these on the flip chart in bold black letters. ‘What else can security mean?’, he provokes, noting the militaristic overtone of the definitions offered by the participants. Someone volunteers that security is also ‘family’; another, ‘love’. Skimming his hand across the growing word cloud, the facilitator motions at the proliferating definitions to argue that security can mean many different things. In a world of violent state centric security measures and proliferating security justifications, talking about security in this safe enough space means reframing what is meant by security, away from securitized discourse towards something closer to the values embodied by the human rights defenders in the room. The facilitator goes on to offer a symbolic intervention into the word ‘security’, suggesting that the word could be replaced with the phrase: ‘wellbeing in action’.

This activity above is the first of many designed to converge the group of human rights defenders around a shared language to discuss danger and uncertainty; as he solicits stories of activism and danger from the group; as he introduces the idea of ‘risk assessment’; as he introduces tools and techniques to deal with surveillance, intrusion, physical danger, and trauma, and finally, as he has the participants create ‘security plans’ to take back and advocate for at their respective organizations. The goal is to come to a common understanding of effective surveillance countermeasures by together defining problems, setting priorities, and building trust. This common language will allow their experiences to become fodder for a decision-making heuristic.

II. Enumerating threat uncertainties and potential solutions

Having 'created a space', established expectations, and introduced a language through which to discuss security matters, the work of maintaining this space continues as a training progresses. 'Creating the space isn't something that I do once and then it's always there and then we do something else', one interviewed trainer reminds (Interview #9). Instead, he argues, it is necessary to 'maintain a realm in which it is possible to understand your surroundings and then do something about it'. To maintain such a realm, the facilitator aims to 'interrogate the surroundings together' through an exploratory process designed to draw out stories about concerning security incidents. Participants are asked to make a diary chronicling the technologies they use throughout a typical day. Each person writes down what they do in the morning, afternoon and evening, punctuating the day's events with descriptions of the use of platforms and devices (Facebook, Instagram, phones and laptops) as well as how they feel at different moments – whether fear, anxiety, happiness or excitement. Now the trainer asks participants to go down this list one more time and take stock of where their technological use creates vulnerabilities or exposes them to danger.

Following this activity, the facilitator asks if people would like to share anything from their diaries. This question is used as a springboard to talk about the different (and similar) threats faced across this international group of people. The goal is to surface stories, perceptions, shared definitions pinpoint common threads, and fuse this together within a comprehensive picture of threats at hand and potential threats in the future. Hong calls this a process of engaging in 'cobbling what we know and suspect into a picture of a sensible, working world' (2015: 73). The participants share their direct experiences with different forms of intrusive monitoring, data breaches, data theft, data loss, and harassment. They speculate about potential adversaries, including the local police; jealous colleagues; controlling partners; and security agencies. From the trainer, participants seek clarification about suspicious phenomena and ‘mystery problems’ that might indicate potential security compromise, including suddenly slow computers and bizarrely blinking screens. This enumeration of uncertainties is the first step towards corroborating or dispelling concern about anomalous phenomena. The facilitator, in turn, seeks to find a middle ground between conjecture and ‘known’ threats, discussing the potential capabilities of ‘adversaries’, pointing out where worries shared by the participants might be merited or not, and offering known information about new surveillance technologies and worrying political developments. As participants share their stories, the whiteboard becomes a repository of different incidents and indicators. As the activities above bring together personal experience and ‘factual knowledge’ of surveillance and insecurity into one frame of understanding, an ad-hoc taxonomy of digital concern emerges. This activity concludes the first day of the training.

III. Commensurating problems and solutions: (Enter the risk matrix)

The next morning, the group of participants comes back together to continue the training. At this point, the group is beginning to converge around a set of common concerns. The trainer hence introduces a range of potential ‘solutions’ to these concerns, consisting of commonly recommended digital security mitigations. Over the course of a morning and afternoon, he goes through a slide show discussing email encryption, two-factor authentication, password managers and password management techniques, as well as strategies for safety and anonymity while participating in social media platforms. The goal is to ‘raise awareness’ of possible mitigations, but which of these will be applied, by whom, and for what kind of particular scenario, is left undetermined. This activity takes the totality of day two. On the morning of the third day, the trainer takes a marker to a long sheet of paper hung from one of the walls of the conference room, drawing a basic grid. It is time to map problems to appropriate solutions. This grid will become what is called a risk matrix. As Jordan et al., (2016) describe, risk matrices 'depict risks within a Cartesian coordinate system' (46)...'classifying risks along two axes, the probability of the risk's occurrence and the severity of its consequences, its potential 'impact'(41). The trainer tells the participants that 'what you need to build is three dimensions of what you can do, what you cannot do or influence, and what you can definitely not do but you can seek help for'. These categories, he explains to me in an interview later, represent 'shades of grey' intended to help people discern the degree of control possible in a given situation, which he underlines can change at any time: 'things are dynamic so they move from one dimension to another' (Interview #9). Still, the matrix' boxes help compartmentalize unwieldy concerns. 'The aim is to eventually have more and more domains under your control or to understand what needs to be done to enable that to happen' (Interview #9).

Writing about the history of the risk matrix, Jordan et al. (2016) note that 'appearing only since the 1980s, risk matrices have quickly pervaded diverse practice fields and have become the most popular technology of risk presentation in practice'(50). Risk matrices 'act as mediating, inter-discursive instruments that translate complex themes into everyday discourse' (41). As such, they are a 'technology of normality' which: 'set borders between normal and abnormal, or...between tolerable and intolerable'(pp. 41). This space of action 'between the tolerable and intolerable' is what the trainer seeks to map out on a sheet of butcher paper. The trainer makes an addition to the classic risk matrix format, however. In addition to creating a cartesian axis which plots out potential future security events by varying degrees of impact and probability, he teases out, together with the human rights defenders, what actions can and cannot be taken in response to identified risks at an individual, organizational and community level. As part of the exercise of filling out the grid, the trainer asks the group of human rights defenders to imagine what kinds of institutional support and structural change must happen for risks currently unaddressable to become risks that can be acted upon. In adding this criteria to classic impact and severity schema of the risk matrix genre, the trainer intervenes into tropes of risk management which serve to make tackling risk entirely the responsibility of the subject *at risk*. The risks that can't be tackled by individuals, organizations, and communities are just as important to represent as the ones that can be tackled, the trainer explains in our interview later.

There is another particularity of the risk matrix constructed by this trainer: unlike many other calculative risk schemas, this risk matrix does not contain any numerical elements and offers no quantitative product or end result. Instead, the cartesian coordinate system drawn up by the trainer is smattered with ideas for security practices such as 'encrypting communications'; purchasing distributed denial of service (DDOS) defence services'; setting up a data back up system; and 'coordinating with other local organizations'. Jordan et al., (2016) confirm the appeal of flexibility between qualitative and quantitative schemas of risk calculation: 'unlike the notion of a 'calculative' risk', they write, 'mathematically correct and precise measurement is not presented as highly important' (45). The use of the risk matrix transports the mess of life into the realm of numbers, metrics, and formal comparison. But though it draws on the language of probability to outline the normal, abnormal; tolerable and intolerable, it fails to adhere to conventional ideas of calculative and statistical reasoning, demonstrating that the social process of making phenomena comparative and equivalent does not always result in a numbered product, even if the aura of numbers is utilized to make up a shared idea of risk. The risk matrix does, however, produce a 'calculation grammar' (Ballestero, 2015) – a common language of valuation, which stands at abstract remove of the 'mess' of information and data brought into the training space. This calculation grammar is used to for further decision making within the remaining time in the training and beyond.

For the remainder of the training, the participating human rights defenders are asked to spend time installing the security mitigations that the trainer has introduced. Furthermore, they are asked by the trainer to create an individual ‘security plan’ which should incorporate relevant and appropriate mitigations into the rhythms particular to their life beyond the training. This integration becomes the link between the temporarily safe space of the training and the uncertain world beyond. However, it is unclear to the extent that this integration will be feasible. After a long fourth day spent learning different encryption tools, one human rights defender confides in an interview with me that though she has now taken part in several security trainings, she has not yet succeeded in integrating most of the mitigations she had been introduced to back into her work. As my prior work shows, the application and integration of security mitigations back into daily life beyond the training space is exceedingly difficult for a number of reasons, from the brittle nature of the software meant to serve as mitigations; to the time and attention necessary to keep them updated and configured ‘correctly’; to the expectations and demands of colleagues back home. If there is funding for it, the trainer will continue to stay in touch with the participants – but often, there is not. For now, it is time to head back out into an uncertain world. As the participating human rights defenders do so, they leave having converged with the other participants and the trainer around a particular language through which to think through the dangers and harms which may come. Whether this language is useful is yet to be determined.

Conclusion

This chapter has explored calculative convergence as a way to understand the processual, intersubjective dimensions of risk assessment in the context of a digital security training. I drew on Callon, Law, and Cochoy's concept of qualculation to develop my own concept of qualculative convergence. I used this concept to build an understanding of how human rights defenders and digital security trainers make sense of surveillance uncertainties and 'tame' them. In describing a digital security training, I showed how the human rights defender participants engage in the valuation of their experiences with surveillance through a myriad tactics which, drawing on the language of numbers and statistics, aimed to make manageable 'risks' out of uncertain circumstances. I explored how this process was enacted across several stages of discussion and practice between a digital security trainer and human rights defender participants. I described these stages as: I. 'Creating the space; II. 'Enumerating threat uncertainties and potential solutions; and III. 'Commensurating problems and solutions'. In the first stage, a safe space was constructed by the trainer, who also established a set of common definitions among participants, useful to discuss and break down uncertainty. In the second stage, personal experiences with danger and uncertainty were surfaced, discussed, and weighed against 'known' information about threats and dangers. In the third stage, concerns were mapped to potential solutions, and henceforth commensurated within a common risk heuristic designed to facilitate decision making.

I show that the push towards a common notion of risk infuses the social process of the digital security training with the promise of order, within an arena otherwise felt to be arbitrary, violent, and messy. On the other hand, I also show that the practice of risk judgement and risk-based decision making is itself messy; spilling over narrow frames of 'rationality' and 'accuracy' and refusing to conform to a corporatist notion of risks out there in the world. In demonstrating the messy transformation of uncertainty into risk, I contribute empirical richness to Callon, Cochoy, and Law's theoretical re-conceptualization of calculation. Furthermore, I augment their theory by bringing qualculation to the realm of security practice. In exploring how uncertainty becomes risk through qualculative means, this chapter also contributes to the advancement of a richer understanding of how people make sense of datafication through different forms of calculative (or rather, qualculative) logics. Finally, in exploring how targeted communities such as human rights defenders apply risk-centric logics to their work, the chapter brings long-standing concerns around risk and security practices within critical security studies into the study of civil society approaches to security risk.

Chapter 7. Infrastructuring the future(s) of cybersecurity: Towards fully automated anticipation?[19]

19 This chapter has been submitted as an article for peer review in July, 2021

Abstract

At a time in which the practices and institutions of 'cybersecurity' are increasingly bounded and consolidated through global governance mechanisms, weaponized in the '5fth dimension of warfare', and enacted through automated, data-driven systems, this chapter aims to contribute to the questioning of the hegemonic logics embedded into contemporary configurations of cybersecurity. Through multi-sited ethnographic study based on four years of fieldwork, this chapter provides a multi-perspectival account of *security infrastructuring* amongst community organizers, technical security providers and non-profit organizations responding to the threat of digital intrusions, surveillance, and online harassment. The chapter looks at how coordination amongst heterogeneous communities of security practice leads to the refraction of anticipatory, data-driven logics of contemporary security across data infrastructures. The chapter introduces the concept of an 'anticipatory security infrastructure' – an information infrastructure which facilitates the collection, processing and analysis of data in order to anticipate harmful future security events.

Keywords: cybersecurity, digital security, data governance, automation, AI, activism, civil society, feminism

Introduction

One day in 2014, the staff of a women's and LGBTQIA+ rights[20] group based in a country formerly part of the Soviet Union were tipped off to an alarming video spreading through online social networks by a pseudonymous youtube account. The video contained a montage of sensitive photographs exfiltrated from the private Facebook accounts of the organization staff. As the photos faded in and out of the montage, the distorted voice of the video's narrator accused the organization of undermining the traditional family values of the country, part of a broader disinformation campaign that took them by surprise. Following an unsuccessful request for assistance from local authorities, the group called together several local organizations working on women's and LGBTQIA+ rights to discuss the attacks. They learned that they were all experiencing similar forms of targeting. However, they were unsure of who the perpetrators were, nor could they anticipate their next moves. In response to the attacks, they began to collectively document concerning digital security 'incidents' through an improvised infrastructure. The goal was to identify patterns in perpetrator actions, predict their future plans, and plan mitigations in response. With few resources and an urgent need to act, the group used the Facebook platform, which it already relied upon for its organizing and community building activities, to collectively track and analyse concerning security incidents through 'secret message groups'. Together they tracked suspected telecommunications surveillance, threats of violence and instances of online harassment. As the months wore on, the organizations became increasingly invested in tracking and documenting these incidents, eventually doing so in 24-hour shifts. The anticipatory labor of vigilance and incident tracking solidified within what I term an 'anticipatory security infrastructure' – an information

20 LGBTQIA+ stands for Lesbian, Gay, Bi, Trans, Queer, Intersex, and Asexual. It is used as an umbrella term used to describe a number of interrelated communities and identities related to sexuality and gender.

infrastructure which facilitates the collection, processing and analysis of data in order to anticipate harmful future security events.

Recently, scholars have explored 'anticipatory infrastructures' in the context of journalism; bitcoin; and energy grids, respectively (Ananny and Finn, 2020; Enslev et al., 2018; Ulfstjerne, 2020). This chapter brings the study of anticipatory infrastructures to the contested realms of civil society digital security and state and corporate cybersecurity, drawing conceptually on critical histories of cybersecurity, 'relational' studies of infrastructure, and studies interrogating the future-driven logics and practices of state and corporate security. The chapter introduces the concept of 'anticipatory security infrastructures' as information infrastructures which result from contestations and collaborations between diverging communities of security practice. While the infrastructure developed by the women's and LGBTQIA+ rights groups introduced above was confined to a small group of people, arose in a moment of crisis, and creatively re-appropriated the existing affordances of Facebook's commercial platform, this chapter explores attempts by digital security specialists working with civil society groups to standardise, centralise, and automate such anticipatory security infrastructures in order to facilitate efficient and 'rapid' response to 'digital threats' at global, trans-regional and local levels. Through a multi-sited ethnographic study of infrastructure (c.f. Star, 1999) based on four years of fieldwork and interviews, the chapter provides a multi-perspectival account of *security infrastructuring* amongst activists, community organizers, technical security providers and nongovernmental organizations (NGOs) responding to 'digital threats', looking at how interaction amongst heterogeneous communities of security practice leads to the refraction of anticipatory, data-driven logics of contemporary security across data infrastructures.

In providing such an account of security infrastructuring, the chapter aims to contribute to academic and practitioner efforts questioning the hegemonic logics embedded into contemporary configurations of security. At a time in which the practices and institutions of ‘cybersecurity’ are increasingly bounded and consolidated through global governance mechanisms (Morgus et al., 2015; Slayton, 2020), weaponized in the ‘5fth dimension of warfare’ (Cavelty, 2013; Dyer-Witheford and Matviyenko, 2019), and enacted through automated, data-driven systems (Amoore, 2020; Dwyer, 2019; Bellanova and de Goede, 2020) it bears reminding that security is a fundamentally open-ended and irreducible concept, practice, and goal articulated through vastly different epistemologies and moires (Fichtner; 2018; Hansen and Nissenbaum, 2009; Nissenbaum, 2005). While the international relations of cybersecurity play out in high-level policy fora, security practices, standards, and infrastructures are articulated through daily practice (Ermoshna and Musiani, 2018; Kazansky and Milan, 2021; Monsees, 2020) as well as attending cycles of infrastructure maintenance and innovation (Bellanova and de Goede, 2020; Slayton and Clarke, 2020). Scholars, activists, and community organisers have worked to ‘reconfigure security’ (Reconfigure Network, 2021) to take account of its hegemonic logics, pushing for practitioners and policy makers to bring cybersecurity in line with human rights frameworks, anti-racist commitments, and gendered considerations (Brown D and Pytlak, A (2020); Coding Rights, year; Hackblossom, n.d.; Kazansky, 2015; Millar, et al., 2021; Petty et al., 2018; Slupska, 2019; Tactical Tech, 2016; Tanczer et al., 2018). Towards the de-centring of state and corporate cybersecurity narratives, the chapter calls attention to the way that security standards and infrastructures arise not just from hegemonic state and corporate security actors, but through friction-full ‘governance from below’ (c.f. Lea and Stenson, 2007) lead by civil society actors.

The plan of the chapter is such: in the next section, I contextualize concerns with anticipation and security infrastructures in the literature. Following this, I explain my research methods. I then introduce efforts by civil society digital security practitioners to more rapidly respond to digital threats. The chapter then introduces and investigates the practices of three groups and individuals engaged at the cross-sections of divergent security infrastructuring approaches, looking at the 'frictions' of security standards-setting and anticipation across an 'institutional ecology' of digital security rapid response. The chapter concludes with questions for further research.

Situating Anticipatory Security Infrastructures

This chapter studies processes which 'infrastructurally encode anticipation' (paraphrasing Ananny and Finn, 2020: 1604) at the intersection of security specialist repertoires and NGOs and grassroots groups experiencing 'digital threats'. Towards the investigation of security infrastructuring, the chapter builds on two areas of study: first, it draws on information studies literature exploring digital and data infrastructures as processual, diffuse, and heterogeneous entities built and maintained through the interaction of communities; and second, it looks to critical and historical studies of security to help contextualize the digital security practices of civil society. This section draws on the above to contextualise three main areas of concern for this chapter: anticipation, infrastructure, and digital security.

'Anticipation' refers to future-oriented modes of action which intervene against potential undesirable security outcomes (c.f. Adams et al., 2009; Anderson 2007; 2010; Kazansky 2021; Pink et al., 2018). As framed in this chapter, anticipatory security action emerges from a heterogeneous milieu of practices, drawing from data intensive and algorithmic prediction regimes as well as intuitive pattern-finding and sense-making practices. This framing builds on my findings in Chapter 4, where I explored anticipation as it is enacted through the practices of security specialists working beyond corporate and state structures. In this chapter, I showed that 'anticipatory data practices' draw from a number of different culturally specific histories of risk, modelling, preemption, and prevention of undesirable futures. I also argued that anticipation can be understood as a thread which ties the interactional dynamic so-called 'dance of surveillance' (Marx, 2009) together. Per Clarke (2015), anticipatory modes are a kind of interstitial 'articulation work' which help give shape to sociotechnical assemblages. In this chapter, I build on Clarke's notion of anticipation as infrastructure articulation work to show how anticipatory modes serve as a driving force of the maintenance and development cycles that shape security infrastructures. These themselves arise from ongoing interaction of surveilling and intruding actors and those who build infrastructures to withstand against, recover from, or 'neutralize' (c.f. Marx, 2009; Wood and Thomson, 2018) their actions through security measures.

'Digital security', as scoped by interviewees, is a broad term used to refer to civil society repertories for safety from different forms of data exploitation, harassment and targeting, and security intrusions by states, corporations, and affiliated actors. The chapter contextualises digital security practices and infrastructures in relation to commercial and state cybersecurity, showing the porousness of these overlapping communities of practice and how civil society's digital security practices are shaped by values articulated through agonistic interactions between groups of varied institutionalization, geographic location, issue scope. As I argue across the chapters of this thesis, civil society challenges and reconfigures hegemonic notions of security while also appropriating the logics and practices of hegemonic actors (see in particular Chapter 4 and 5). The chapter studies this appropriation and reconfiguration through the lens of a porous 'institutional ecology' (Star and Grisemer, 1989) attuned to the agonistic relations of civil society organizations, security specialists, grassroots movements, and technologies brought to bear against digital threats (c.f. Mouffe, 2013; Horgan and Dourish, 2018). Looking at the infrastructural politics of data collection, analysis, standardization, and automation, I draw upon work that studies information infrastructures as contingent and processual, bound up in continuous construction and entropy (Star, 1999; Bowker and Star, 1999).

As Bellanova and de Goede (2020) point out, ‘data infrastructures are not neutral, as they materially, legally and politically support specific ways of doing security’(13). Clark-Ginsberg and Slayton (2017) point to the processural way that these ‘ways of doing security’ emerge, highlighting that contemporary cybersecurity infrastructures are ‘the embodiment of a cacophony of overlapping and congruent standards’ (2) which result from decades-long struggles at local, regional, and global levels. In this chapter, I will show that digital security infrastructures emerge through conflicting ways of doing security, and as such, may be more ‘seamful’(Vertesi, 2014) than congruent. Specifically, the chapter identifies an important friction between what I identify as two overlapping yet divergent approaches to digital security rapid response and infrastructural security anticipation. The first – a ‘global’ approach encourages increased threat data standardization and automation across globalized, centralized data super-structures, while a second - ‘local’ approach encourages community-driven and ‘autonomous’ – not to be confused with automated – security through localized data infrastructures and practices which challenge state and corporate driven security definitions. Taking a processural and relational perspective on anticipatory security infrastructures (c.f. Star, 1999) this chapter looks at how the friction between these two identified approaches contributes towards the making and un-making of cyber and digital security standards and infrastructures, honing in on data standardization conflicts, infrastructural politics and anticipatory logics imbricated in the struggle to respond rapidly to ‘digital threats’. In exploring the tension between two approaches to digital security and attending contestations, I draw on Star and Bowker’s notion of imperialism (Star and Bowker, 2007) to characterize the power-laden conflicts that arise in the development of security metrics, standards, and classification schemes. The chapter investigates what emerges from the push and pull of these two approaches, analyzing their significance amidst broader discussions of security, data, and automation.

Methods

The study is concerned in particular with an international 'ecology' (c.f. Star and Griesemer, 1989) of non-governmental and grassroots groups which, through collaborations and contestations, develop an ever-evolving repertoire of mitigations for digital threats. The analysis in this chapter draws from a larger multi-sited, qualitative study of civil society responses to the shifting threats of digital surveillance and datafication. In total, 50 interviews were conducted with digital security, digital rights, and Internet freedom practitioners between 2016 and 2019. Interviewees were selected at 12 international digital rights and Internet freedom meetings in Europe and Southeast Asia, where participant observation was also conducted. Interviewees came from 26 countries in different regions of the world. Their diffuse geographical representation results from the international nature of the conferences where fieldwork was conducted, which are explicitly organized to bring transnationally coordinating civil society actors from across different regions together for discussions. The transnationality at play connects directly to this chapter's interest in exploring friction-full governance from below, which emerges from overlaps and divergences on the basis of community priorities, geography, culture, and resource equity and inequity. Participant observation took place at public discussions about digital security rapid response, where digital security specialists, technical service providers, NGO workers and grassroots organisers engaged in frank discussion about emerging best practices, shortcomings of 'digital security support', and emerging priorities for the 'field'. The struggle to coordinate rapidly against digital threats emerged as a recurring theme in inductive analysis of initial interviews and field observation, which lead 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 grassroots groups, and cybersecurity technicians and service providers working with both civil society organizations, companies, and governments. The fieldwork and interviews as a whole 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.

Rapid response to digital threats: from threat indicator to anticipatory infrastructure

As 'digital threats' have become commonplace, civil society organizations around the world have sought to develop standardized protocols and coordination mechanisms to respond rapidly in the wake of security 'incidents'. A borrowed term from the fields of emergency medicine and humanitarianism, 'rapid response' is closely related to the 'computer security emergency response' practices of commercial and state cybersecurity (see: Morgus et al., 2015; Slayton and Clark, 2020). Within civil society's 'digital security ecosystem', as it is referred to by practitioners (the Engine Room, 2018), rapid response refers to a repertoire of services providing technical support for urgent digital security issues, ranging from suspected malware attacks, website compromise, distributed denial of service attacks, data exfiltration, and data loss. The focus is on mitigating the threats faced by human rights and social justice nonprofits and grassroots social movements, a gap left largely unaddressed by commercial and state security enterprises (Maschmeyer et al., 2020; Millar, 2021). Though 'rapid *response*' implies action taken to counter the effects of a concerning event, interviewees underline that responding rapidly requires having the correct mitigations and resources already in place beforehand.

This need for preparedness engenders a future-oriented approach to security (c.f. Amoore, 2020; Anderson 2010; Aradau and Blanke, 2017; de Goede, 2012). As an interviewed digital security specialist explained it 'being able to know what is going to happen is a way to find out where to put resources in the future' (Interview #42). Importantly, however, none of the security specialists interviewed believed it is possible to 'predict' digital threats with precision or accuracy, nor is that the goal. As another specialist explained, 'sometimes people are super worried because they don't know if the threat is going to happen and its really hard to say yeah there is 80 percent chance (Interview #41). On the other hand, a third security specialist offered: 'when you know enough about what happened in the past with threats you can probably figure out whats going to happen in the future or at least have an idea of how it will evolve' (Interview #29). In other words, preparedness becomes possible by tracking and finding patterns in data relating to past concerning events – and from this past data, extrapolating likely future threats. I argue that this 'loose' approach to prediction is best understood as a form of anticipation – a concept open ended enough to capture the messiness and heterogeneity of judgement and decision making enacted through future-oriented security, or, 'anticipatory security', defined here as a future-focused modality of security enacted through vigilance and data-driven practice.

Anticipatory security, as scoped by interviewed rapid response actors, requires continued pattern finding relating to past recorded events, scanning for emergent 'anomalies' (c.f. Aradau, 2018), and engaging in conjecture about potential future attacks. These different modes of analysis rest on the availability of threat-related information, which includes organizational documentation of incidents pertaining to perpetrators and their ‘tactics, techniques and procedures’ (TTP); ‘indicators of compromise’ (IOCs); cybersecurity bulletins and alerts, research reports issued by anti-virus vendors and academic institutions documenting new vulnerabilities and attacks, and ‘threat intelligence’ collected on trends and attack patterns within specific sectors and communities at global, regional, and local levels. Interviewees highlighted that despite these many potential sources of threat information, ‘actionable’ and ‘reliable’ threat information is challenging to come by. One reason is the ephemerality of many kinds of digital attacks, which makes threat perception, identification, and data capture a difficult proposition. As one security specialist explained, ‘there is no click click anymore when your phone is tapped’ (Interview #12). In many cases, there may very well be residue left on devices and infrastructures that would constitute ‘evidence of compromise’ but recognizing and capturing it requires deep technical specialization out of reach for many NGOs and grassroots groups.

Still, the ‘burden of proof’ regarding threats and harms is placed upon the communities experiencing them, as per the case of the women’s and LGBTQIA+ rights activists of the chapter’s opening vignette. This kind of responsibilisation puts human rights defenders, community organizers, and NGOs to work vigilantly documenting suspicious anomalies (c.f. Kazansky, 2015). Interviewed security specialists thus promote the practices of documenting ‘everything’ in case it might reveal a concerning pattern of phenomena indicative of compromise. As a security specialist teaching documentation techniques to grassroots groups put it, ‘it’s very simple actually…. just document everything that happens’ (Interview #37). Another such specialist underlined: ‘whenever there is an incident we always write it down’(Interview #39). Though in commercial and state cybersecurity, threat monitoring efforts aim to obtain granular forensic data and are increasingly enacted through automated ‘security sensing’ devices such as network monitoring tools and intrusion detection services, interviewed specialists working with NGOs and grassroots groups argue that documentation about potential threats can be a ‘low tech or even no-tech measure’ aimed at capturing experiential, circumstantial, and ‘unstructured’ data (Interview #12). For example, the specialists above prescribe the use of paper diaries to human rights defenders and activists in order record any kind of anomalous event occurring amidst daily life, ranging from the observation of a suddenly slowed computer to a suspicious parked car outside an office, urging also that activists and human rights defenders share this circumstantial data within trusted groups in order to tease out patterns indicative of compromise or danger.

The combined necessity to document, analyse, share and compare threat related information on a continued, anticipatory basis gives rise to information infrastructures to sort a mess of varied threat information ranging from data collected by ‘high-tech’ automated threat scanning platforms to the anomalous experiences recorded in the ‘low-tech’ diaries kept by grassroots groups. These analogue and automated forms of analysis are facilitated through a mix of structured analysis tools and the ‘manual’ effort to collect any and all possible indicators of potential danger and find patterns in them. Through an entanglement of so-called ‘automated’ and ‘human’ judgement, they enact what Dwyer (2019) calls a ‘more-than-human sensing’ of security threats (118). Multi-sited, and ‘seamful’ (Vertesi, 2014), these anticipatory security infrastructures may (or may not) stretch across geographic borders and communities of practice, centralized and decentralized databases, and varied forms of sensing devices. Though flexible and geographically fluid, they are also contingent and brittle, agglomerating and breaking through the social frictions and attending cycles of maintenance and innovation (Clark-Ginsberg and Slayton, 2017). As Bellanova and de Goede (2020) summarize, security infrastructures ‘require encoding, standardizing, tinkering, and tailoring’ (5). The next sections of this chapter focus on these processural politics of anticipatory *infrastructuring*, as enacted through coordination between large NGOs, grassroots groups, and commercial actors trying to respond 'rapidly' to threats.

The geographies and institutional ecologies of anticipatory security infrastructuring

This chapter differentiates between three broad categories of actors whose agonistic politics help make and unmake anticipatory security infrastructures. First, the chapter places into one category 'global' rapid response actors: large NGOs with a global or trans-regional scope of work on digital rights, Internet freedom, and digital security. Predominantly based in Northwestern Europe and North America, they have historically dominated agenda-setting in the field and have presided over the majority of funds and technical resources (Brooks, 2019; Kazansky, 2021). The 'global' approach to rapid response has relied upon centralized forms of governance. For example, several global organizations run global emergency hot lines and 'help desks' to which constituents can call or send messages from any timezone and ideally be able to a representative at short notice. As explained in my interviews and hashed out at observed rapid response meetings, sometimes a global organization addresses incoming 'support' cases itself. However, if staff lack resources or time, the organization instead matches the constituent in search of support to the organization's network of specialists distributed across the world. Global rapid response actors promote mechanisms for large scale threat information sharing across communities and regions, arguing that such scaled-up information sharing processes can enable civil society to collectively identify and track common threat patterns and respond with increased coordination and efficiency. As I show, the imagined ideal for such threat-information sharing processes is a birds eye view of digital threats facing civil society around the world – seen as a powerful tool to ‘proactively’ anticipate and prepare for future threats. As I further show, the desire to work at such a scale creates an imperative to automate security work – an imperative Slayton documents in the history of state and commercial security as well (2015).

A second category of actors is distinguished by their particular issue focus and/or ‘localized’ geographic scope, working in local or trans-local configurations to address the security concerns of human rights defenders and other constituent communities. Interviewees from North America, Central America, the Eastern Horn of Africa, South Asia, Southeast Asia, and Post-soviet Eurasia are represented in this study. Issue-focused communities work to end violence against women, advance LGBTQIA+ rights, sex worker rights, anti-racism, land and environmental rights, and anti-corruption, among other allied issues related to social justice, Internet freedom, digital rights, and human rights. Historically these organizations and grassroots groups have had less access to digital security related financial resources or specialised assistance, relying often on services disbursed on a voluntary basis by global non-profit rapid response actors and both nonprofit and commerical technical service providers. As my interviews and fieldwork will show, amidst a push by NGOs to centralize and standardize security knowledge and expertise, a number of local rapid response actors have pushed back against the globalised approach, choosing instead to keep their threat information confidential and ‘unstructured’. One reason for this is a distrust of ‘cybersecurity’ as defined by state and corporate actors, which in many cases plays out orthogonally to the interests of social movements through surveillance and monitoring of their activities (see: Amoore, 2020). Thus, a requirement to homogenize and share data could be considered a violent act of ‘imperialism’ as Star and Bowker (2007) characterize the violent processes of standardization undergone towards the advancement of information and classification infrastructures. Though local organizations run emergency hotlines and help desks as well, they are run at a smaller scale. In fact, a number of interviewed local actors push back on the idea that a uniform or scaleable model for rapid response is possible, calling instead for the recognition of the legitimacy of heterogeneous security approaches.

The third category of rapid response actor involved in civil society rapid response consists of commercial and state cybersecurity teams and technical service providers who civil society organizations regularly reach out to in order to gain redress with social media platform content takedowns, recovery from Distributed Denial of Service attacks, and other common cybersecurity issues. In their practical role amidst emergencies, commercial and state actors require and request data from the digital devices of NGOs and grassroots groups to conduct their investigations, pinpoint perpetrators, and gather evidence of security compromise. Having been steeped for decades in the minutiae of technical standards and terms of art, these actors exert an influence on the standards-setting and infrastructuring now taking place across the digital security rapid response ecosystem. This influence occurs both in direct interactions in the midst of 'digital emergencies' as well as in the movements of 'experts' from commercial or state cybersecurity into civil society communities of security practice. One main connector between commercial/state and global 'civil society' actors is a shared anxiety over the 'global' and 'viral' dimensions of digital threats (c.f. Parikka, 2007). In interviews, a recurring theme in discussions for why centralization and standardization of threat information are important is the observation that different communities notice similar patterns of concern, yet lack the language or infrastructure to systematically track them due to a lack of establishment of common 'threat taxonomies' and data standards. This conundrum mirrors the lack of shared language documented by Slayton and Clark (2020) with regards to the early days of computer security incident response at the state level. Slayton and Clark trace how the desire to establish such a language served as the impetus for security standardization, centralization of security infrastructures, and emergence of global cybersecurity governance mechanisms. This shared anxiety produces both collaborations and contestations between unlikely allies.

In the next sections, I follow the work of three individuals and constituent groups involved with civil society digital security rapid response. Following the productive frictions between their approaches to security allows us to explore controversies around whether security infrastructures should be global in scope; how data about security incidents should be classified and processed; with whom should and shouldn't this vital information be shared with; and to what extent security becomes an automated, data-driven enterprise. First, I introduce a security specialist at a large NGO involved in the development of an efficient and standardized security regime; second, I introduce a group of state cybersecurity incident responders who promote threat information sharing and try to collaborate with civil society organizations; and third, I introduce a group of feminist security practitioners who argue for an autonomous – not to be confused with 'automated' – and local approach to digital security.

Civil society security practices: towards common standards and centralized infrastructures?

M has spent several years developing codified practices and infrastructures for the service of civil society's efforts to manage digital threats. He considers himself an enthusiastic proponent of increased threat information collection, standardization, and threat information sharing. Around the time of our meeting in 2018, M was tasked with creating a 'systemic' approach to security for the global development organization he was working for at the time. The main impetus for this strategy was a need to identify and respond to security risks more ‘efficiently’ in order to match the fast-moving and serious nature of digital threats (Interview #12). For M, this efficiency was an impossibility due to a lack of actionable threat information. M argued that while this information does exist ‘in theory’, it was, at the time, hidden in too many places; scattered throughout guides, mailing lists, and internal communications in non-standardized formats. Sitting together at a small table in the courtyard of a digital rights conference venue in 2018, M took me through the ‘workflow’ he was developing to create a more ‘agile’ and ‘efficient’ organisational security strategy. On his laptop, he drew my attention to a database listing hundreds of sources of information on potential past or future security ‘events’ obtained through investigation of potential threat actors and their motivations.

M searches for credible threat intelligence sources on a regular, continued basis, due to a continuously changing ‘threat environment’. One technique he uses to obtain threat intelligence is to manually search on the Internet for ‘publicly available’ information including websites monitoring political situations in regions and countries, antivirus company reports, and bulletins from state cybersecurity teams from across the world. In addition to these ‘public’ sources of threat intelligence information, he also draws upon an enormous amount of information concerning security incidents documented *within* his organization. M copy and pastes all of these threat intelligence sources into an excel spreadsheet containing thousands of URLs, explaining that having this threat information arrayed within one spreadsheet is a starting point for data structuring and standardisation: ‘the document itself adds structure’. Structuring for M involves developing a common ‘threat taxonomy’ through which to order different kinds of threats, threat actors, threat impacts, and potential threat mitigations. This kind of taxonomy will allow him to find patterns in the data, and will more broadly facilitate the standardization of rapid digital threat response.

Through his continuous engagement with the categorization and structuring of these sources of information, M begins to see emergent patterns in the data, attempting to identify concerning patterns in information from public sources and confidential organizational files. The goal is to identify ‘flags’ of concern and to extrapolate a set of ‘indicators’ which will serve as a triggers for action in the event of probable threats: ‘we are trying to determine likelihood. If its likely its going to happen, we will have to mitigate it...what are the swaths of indicators that allow me to make a decision?’ By combining this global threat intelligence with the information ‘local’ to his organization, M tries to obtain a comprehensive view of emerging threat patterns that can enable him to anticipate probable threats. Yet, for a truly comprehensive view, M explains that he needs to find a way to confirm this pattern is more than just his conjecture alone. In his work to standardize security practice, M wants to correlate the data points he collects with that of other organizations across civil society. In cybersecurity terms of art, M wants to engage in ‘threat information sharing’ with other communities conducting similar threat intelligence efforts, pointing to the threat intelligence platforms and communities established by states and corporations as inspiration. Furthermore, M wants to automate and synchronize all the different parts: ‘everything needs to be a dial that you can tweak and where it cascades, so that if an indicator changes you know what else to change across the board.’

Yet to engage in this kind of information sharing in a civil society context – and beyond his own organization – requires three conditions: first, a desire by other organizations and groups to share their own information; second, a common platform on which to do so; and third, a standardized form through which to record and share it on this platform. The following section introduces an effort by one group of state cybersecurity actors to develop a threat intelligence platform which they hope can facilitate the kind of broad information sharing practices M aspires towards within civil society. As I will show, the shared interests, infrastructural meeting points, and divergent epistemes which collide through this effort help shape the course of security standardization and rapid response coordination.

Commercial and state cybersecurity threat intelligence: overlaps and divergences

In 2012, a state-organized team of security incident responders convened a meeting to discuss the state of cybersecurity coordination and threat intelligence at a global scale. As explained by one interviewed member, ‘we had a meeting with other threat intelligence teams to discuss weird stuff we were seeing’ (Interview #29). One of the main outcomes of the meeting was that ‘we noticed how often threats seemingly particular to one sector are in fact common across others’. However, though ‘every team was working on something really similar...we didn’t really want to share our data’, with the result that the teams were altogether ‘just sitting on piles of data’. To make this data actionable, ‘the community really wanted to automate the process as much as possible’. The desire to foster information sharing and automate data sharing across teams ‘was a tipping point’ for the team’s security work, following decades of development of common security standards, threat information taxonomies, platforms through which to comprehensively track threats, and techniques to automate all of these processes. As Slayton (2015) documents through historical analysis, by the mid-1980s, automation was viewed as a key priority in computer security. With work on automation also came the prospect of finally operationalizing ‘real-time’ automated threat monitoring and prediction, a goal first articulated in information security in 1967, at which time the RAND institute had laid out this aim at a prominent conference (24). Nearly 40 years later, techniques of automation had advanced through the availability of big data and new forms of predictive analytics, yet reliable and comprehensive threat information has remained a persistent challenge.

In an effort to understand how to encourage more threat information sharing, the state cybersecurity team 'started to build a small interface to have a way to store indicators of compromise, and give access to people to it to synchronize it' (Interview #29). Each 'user' would create their own 'instance' – or personal area – on the threat intelligence platform. There, they could maintain a collection (called a 'galaxy') of threat information which could be shared controlling how 'far' the information spread share made public, shared with particular communities, or kept confidential. The hope was that the granular information controls provided to imagined threat information sharers would engender trust and confidence in sharing 'sensitive' data, and thus encourage as many different sectors and communities participate as possible – all towards a desired global view of trends in vulnerabilities and attacks. By 2017, the team's small threat intelligence interface had grown into a large online platform designed to allow any motivated security professional or targeted actor to submit threat information in a standardized format and find correlations in the data. The kind of information stored included lists of common domain names associated with malware and forensic digital evidence related to attacks, including files containing executable malware and records of abusive messages sent via email and other communications. Part of the developer team's strategy was to include civil society threat information within their platform. They underlined that at least some of the more 'common kinds of threats pertaining to malware were similar:

> All the NGOs and civil society orgs really receive the same kind of ransomeware that everyone receives...the finance departments at NGOs get the same kind of stuff all kinds of finance departments do. (Interview #29)

If the digital threats faced civil society were similar to those facing banks or commercial institutions, it followed that giving access to civil society could allow the team – and any user of the platform – to identify common attack patterns, contributing to the broader aim of continuous threat monitoring at a global level. Yet, the inclusion of civil society into the platform was far from seamless. In our interview in 2017, one developer of the platform shared his frustration that despite the invitation they made to different civil society organizations to participate in the platform, very few had actually recorded or shared information. Why? Through discussions with civil society digital security practitioners, he and the other developers learned that the lack of participation could be attributed to two issues: first, the continued source of friction around 'trust' again appeared to place a wedge between these overlapping yet divergent communities of security practice. In particular, the developers noted a distrust by civil society organizations towards the idea of sharing security-related information about their organizations and constituents with agnostic security actors operating at the cross-section of several communities of security practice (again, the platform was intended to cater just as much to banks, other corporations, and state institutions, and was configured by a team of security professionals aiming to equally address threats from every sector).

The second issue developers observed was a misalignment around what constitutes a security-related 'indicator' and how 'threat information' should be structured. As introduced earlier in the chapter, for digital security practitioners in civil society, a security-related 'indicator' may constitute any experiential data collected from immediate life and interactions with technologies therein; for example, the perception of 'slow' computers, signs of wiretapping such as clicks; or perceptions of potential physical surveillance, such as being followed by a suspicious car, were considered useful forms of data to track through diaries or secret Facebook groups (per the opening vignette of the chapter). In contrast, the developers were accustomed to working with 'highly structured' data about cybersecurity 'events' classified according to a taxonomy established by cybersecurity governance bodies. This taxonomy of threats predominately concerned ‘indicators of compromise’(IOC), a term to describe structured data about malware, ransomeware, and DDOS attacks, while omitting the kind of experiential data mentioned above. Following this classification scheme, IOCs took the form of suspicious domain names, malware samples, and other forms of ‘forensic data’ extracted from computing processes. This misalignment around what constitutes a security-related indicator, and subsequent inability to participate according to the constraints of the platform, seemed to make data standardization an impossibility, threatening also to preclude its sharing through a centralized platform and frustrating the goal of a global, anticipatory view of cybersecurity threats.

In an effort to resolve the impasses outlined above, the state-led cybersecurity body sought to include a wider breadth of qualitative ‘unstructured’ data that does not abide by established cybersecurity threat taxonomies. This could be added to a new ‘metadata’ form adjacent to the main database where users were to record threat information. Further, the cybersecurity team shifted how it would use the infrastructure it had built in support of civil society. Rather than encouraging ‘civil society’ – in the broadest sense of the term – to use the platform, the team shifted to primarily collaborating with other technical service providers in contact more directly with NGOs and grassroots groups, who both had ready access to threat information due to their provision of services to NGOs and grassroots groups, and were already accustomed to structuring (in other words, ‘translating’) threat-related information in accordance with cybersecurity standards. Beyond the constraints of this platform, however, are more radical visions to be explored, bringing us to the next section of this chapter. While the state cybersecurity team viewed the misalignments between the different imagined users of the threat intelligence platform as an obstacle to ‘effective’, anticipatory security, they can also be understood as a productive friction; an act of principled defiance, and an impetus for the development of *other* kinds of security infrastructures and approaches to threat information, which are explored next.

Feminist counter-practices and local, autonomous security stewardship

In 2018, members from five feminist, women's and LGBTQIA+ rights groups from different countries and regions of the world converged for a trans-regional discussion of how to document and describe digitally related threats and harms in a way that would do justice to survivors of violence, both 'online' and 'offline' (field notes, 2018). In a discussion held at a large digital rights conference in 2018, they explained to the audience that 'mainstream cybersecurity' had yet to account for the concerns of their communities; particularly that contemporary cybersecurity practice predominately omits the 'gendered' concerns and embodied nature of 'digital' harm faced by women and non-binary individuals. This problem extended to the language used to describe threats not just by security specialists but by constituents trying to describe what they were experiencing. As an example, one person who participated in this discussion explained, in our interview after, that it was common for people calling the hotline she ran to try to describe what they were experiencing through the stilted language of 'hacking':

> a lot of people would call in to a helpline and say…oh I've been hacked, and we were like, you are not being hacked, this is blackmailing. Maybe it was through accessing your Facebook account that they got your images that they are using now (Interview #39).

The interviewee argued that 'hacking', along with terms like 'surveillance' and 'compromise', were much too vague and apolitical to describe phenomena such as the targeted attack which this woman had experienced. Vague, apolitical cybersecurity language had practical ramifications for information sharing and data infrastructuring: how could threat information be discussed and shared if the categories created to describe and capture threats did not recognize or describe the nature of the threats they were contending with? Though mainstream threat taxonomies do also contain much more granular descriptors for threats and security-related indicators, the interviewee argued that it was focused predominantly on 'traditional' cybersecurity issues, while barely touching areas related to violence against women (a problem also identified in recent scholarship on tech abuse, e.g: Slupska, 2019; Tanczer, 2018). Just as omission from mainstream threat taxonomies was issue, so were the 'terms of inclusion'(Hoffman, 2020) – in, particular the requirement to conform to state-centric problem definitions. Many interviewees, for example, object to the relatively recent ubiquity of the term 'cybersecurity' due to its militaristic overtones. For this reason, throughout texts, guides, and interventions produced by feminist practitioner organisations produced over a number of years now, pleasure and embodiment are centred as elements of digital security, while fear-driven and patriarchal notions of safety and security are challenged and reframed (Coding rights, n.d.; Cyberseguras, n.d.; Kazansky, 2021; Radloff 2013; 2018; Tactical Technology collective, 2015; 2016).

Hence, the five groups pushed one another to 'dig deeper' and find language that could capture the political context of security threats; embodied experiences of danger; and motivations and end goals of attackers. One interviewed security specialist who participated in the development of the typology explained that to do so, 'we needed to come up with our own terms' (Interview #39). The group who met laid out its primary aims for the typology: first, it should give proper weight to the gendered violence perpetrated through digital platforms against women, women's rights defenders, and LGBTQIA+ communities. To do so would require accounting for the fact that attacks perpetrated 'online' – and resulting harms are rarely confined to the online realm:

> The common message is, this is violence, the same violence that we live, because people use to say 'this is not violence, I did not used to see it like violence', or ' online violence is not real'. So now, the message is, this is the same violence that we

> live in the streets, in our houses, in our beds. This is the same one (Interview #39).

Thus, discussions between organizations focused on how to bring more legitimacy to the idea that online abuse or ‘violence against women online’ is violence regardless of whether it manifests digitally or in ‘meat space’. Rather than simply add new categories of threat to the fixed classification systems of global cybersecurity actors such as the developers of the threat intelligence platform discussed in the previous section, these groups aimed to create a community-centred and relational terminology – referred to as a ‘typology of violence’. In addition to coming up with terms that better matched the nature of community-centric threats, the groups involved made a conscious effort to connect different techniques of cybersecurity threat to the intention behind them, which would more explicitly link techniques of violence (intrusion into personal devices; use of sensitive data without consent; misogynist discourse) to the broader motivations of perpetrators (disinformation campaigns; intimidation; extortion; bodily harm; gaslighting). This relational terminology, they believed, would advance their own efforts to better document and track threats particular to women’s, LGBTQIA+ and feminist groups – but it was not intended for inclusion in globalized cybersecurity infrastructures. The effort by these groups to reframe and redefine security is ongoing, and in the case above, only captures one moment in time in a decades-long struggle. It is, however, paradigmatic of a number of other efforts to decentre, reframe and reconfigure security technologies and governance.

In this section, I highlight one more example illustrative of the productive frictions of a broad and diverse field of security, going to a meeting I observed on the future of rapid response, where the tensions around the global and local dimensions of security work and its appropriate governance came to a head. At the 2018 edition of the same digital rights conference where the women’s, LGBTQIA+ and feminist groups met, a small Southeast Asian organization was asked to present on its experience with responding to the digital support requests of its constituent community. The organization recounted that during its years of reliance on a global organization for security infrastructure support, it had often seen requests for assistance unmet by global rapid response actors due to their lack of capacity and expertise in regional and local issues (field notes, 2018). As a result, the Southeast Asian organization went on to build up its own autonomous approach to digital security rapid response, moving away from centralized information sharing platforms with global data flows and instead building a rapid response helpline intended only for constituents and activists in-country. Because of its demonstrated need for an autonomous and localized approach to rapid response, this organisation and others in attendance expressed a wish for more control over the stewardship of the rapid response ecosystem and how its resources were distributed.

Notably, this request was acknowledged by global rapid response actors present, who responded with a proposal for a new model of governance and coordination. In particular, one high level staffer of a large global NGO proposed moving from a centralized to a 'federated' model of rapid response. Federation would involve delegating more security support tasks to smaller, local actors. To do so, the global organization would 'package [its] learnings' gained from its years as a central rapid response institution into digestible formats and 'push down' well-defined security tasks to locally operating organizations. While the open discussion was welcomed, the proposal was received with controversy. The notion of resource-rich organizations from North America and Western Europe 'pushing down' knowledge to the so-called periphery was called out for its neocolonial overtones. Instead, attendees called for substantive resource redistribution and lateral, community-centric knowledge sharing. This example illustrates that the institutional ecology of rapid response is shifting from a centralised, global model to something other. Towards a re-configuration of the rapid response ecology, large organizations have provided increased support to regional and local infrastructures, viewing this as a positive and necessary development amidst an ever-growing influx of requests for assistance. But who decides what this new configuration will look like, and what are its implications for civil society? This remains an open question at the time of writing.

Conclusion

Through multi-sited ethnographic study of security infrastructure (c.f. Star, 1999), this chapter has provided an account of anticipatory *security infrastructuring* by digital security and cybersecurity practitioners engaged in rapid response. The chapter has shown security infrastructuring to be a contingent and fractious process which results in the challenging of hegemonic security problem definitions, standards, and forms of coordination. The chapter identified a friction between what I identified as two overlapping yet divergent approaches to rapid response and infrastructural threat anticipation, looking at how the friction between these two approaches contributed towards the making and un-making of security standards and infrastructures. This chapter thus shows that cybersecurity governance is not just the domain of state and corporate actors, but is negotiated through continued contestation amongst communities of practice ranging from the state and corporation to civil society, which have overlapping and oft-conflicting goals. In an effort to de-centre state and corporate-centric narratives of cybersecurity, the chapter illuminated the importance of feminist counter-practices and local forms of infrastructuring which resist globalized operationalizations of infrastructured anticipation.

In the time since the fieldwork for this chapter came to a close, many changes have come to bear on rapid response priorities and infrastructural configurations. Despite efforts made to move away from centralized models cyber and digital security, the pull of the idealized, ‘global’, anticipatory view of security threats continues to exert a force on the practices and infrastructures of civil society digital security rapid response. In a virtual webinar hosted during the first months of the COVID-19 pandemic in 2020, one global NGO involved in coordinating rapid response efforts at a transnational level invited in a commercial cybersecurity company to give a presentation on how NGOs can benefit from its automated, predictive threat intelligence services. The selling point: where anticipating threats is an eternally difficult proposition, why not let artificial intelligence do the work? At a moment of heightened datafication and ‘totalitarian zoomification’ (Gürses and Rocha, 2021), we can see that the eternal promises of automation continue to illuminate particular futures of cybersecurity. On the one hand, automation seems to offer a way to lessen the unjust burdens of security placed on communities in harms way. On the other, critical debates about AI and datafication show that automated systems can also be productive of insecurity and harm. To what extent civil society approaches to digital security will converge with commercial and state models of automated, AI-driven security is left open to future research. For now, this chapter makes clear that alternate approaches to security and anticipation are important to consider further within broader discussions of security, data, automation, and human agency. As the article shows, even if people ‘internalise [hegemonic] regimes of anticipation through technical practices’ (Mackenzie, 2013: 391), people can also disrupt these regimes by pushing back against the way particular organizations, institutions, and sectors configure security.

Chapter 8:[21] Preventing Preemption: Exploring 'proactive' strategies to counter anticipatory surveillance regimes

21 This chapter has been submitted for peer review in July, 2021

Abstract

This chapter explores how preemptive surveillance is countered, interrupted, and co-opted by targeted communities in their daily work and organizing strategies. Drawing on findings from a four-year qualitative study of resistance to surveillance amongst transnationally networked NGOs and grassroots groups, the chapter constitutes an empirical and theoretical exploration of the imperative for affected communities to *proactively* act *before* violent preemptive surveillance driven measures can exert harmful effects. The chapter investigates how the orientation towards proactivity influences security/safety practice and community organizing work, looking particularly at the proactivity of data-driven *resilience* and abolitionist *refusal* in human rights and social justice organizing work. The analysis of proactivity – defined here as the imperative to act before probable harm from preemptive violence – provides insight into the potentials of resistance to what Mackenzie calls an 'anticipatory regime' (Mackenzie, 2013) of contemporary surveillance and policing.

Keywords: predictive policing, preemption, abolition, refusal, resilience, digital security, automated systems, temporality

Introduction

‘Before the bullet hits the body’ is the title of an incisive research report published by the grassroots US abolitionist group STOP LAPD Spying Coalition (SLSC)[22]. The report breaks down the problematics of predictive policing in Los Angeles and pushes for the urgent abolition of the ‘Stalker State’ (STOP LAPD Spying Coalition, 2018). The title of the report, according to an interviewed community organizer and volunteer, emerged from the many meetings during which the group worked through strategies to support poor, unhoused, immigrant, Brown and Black communities put at the sharp edge of oppressive policing measures in Los Angeles. Since 2010, the city of Los Angeles has been a central site of contestation around the harms of predictive policing (Brayne, 2017; 2020), a paradigm of policing characterized by the use of data-driven techniques to preemptively surveil suspected individuals, communities, and their surrounds (Andrejevic 2017; Petty et al., 2018; Williams, 2019). Responding to the automated forms of preemption at play in the ‘intelligence-led policing’ programs of the Los Angeles Police Force, the title of the SLSC report has a dual meaning. First, it refers to the police force’s imperative to preempt criminality through actions that have resulted in well-documented cases of policing abuse. Second, it refers to the SLSC’s urgent imperative to prevent further harm to its constituent communities at the hands of the police. Reflecting on the work entailed in countering the harms of preemptive surveillance in Los Angeles, the volunteer organizer explained that saving lives within an environment punctuated by danger and repeated loss meant ‘acting

22 LAPD stands for the Los Angeles Police Department

proactively...realizing that my fight wasn't just the aftermath but the before' (Interview #43).

This chapter explores the 'before' and its spatial-temporal logics as the site of contestation around preemptive regimes of surveillance. The 'before' or the 'not yet' (Dencik et al., 2018) is a 'time/space of preparedness'(Aradau and van Munster, 2012). 'Acting on the time before', writes Massumi (2015: preface) is the 'operative logic' of violently preemptive actions taken by powerful actors (viii). While the existing literature focuses on the actions of policing and security actors, SLSC's work organizing against predictive policing harms shows that countering the harms of preemptive action also implies 'acting on the before' – to disrupt what Sheehey (2019) characterizes as the paranoid and racialized temporality of policing. The before, per the interviewed SLSC organizer, is a vital pocket of indeterminacy and a buffer against the violent injunction of systems which aim to control and narrow future(s), which must be harnessed and defended by communities through 'proactive' strategies of safety. Looking beyond the experiences of SLSC, the need to act *proactively* against anticipated surveillance and data-related harms is a central theme arising in the interviews and field work conducted in my four-year study of surveillance resistant practices and infrastructures in the context of civil society and social movement efforts to advance the cause of data justice[23].

23 In this chapter, 'civil society' and 'movements' are terms used describe how the people who are featured in this chapter respectively describe their communities. While interrelated and often overlapping, the groups and individuals interviewed here often make a meaningful distinction between the NGO-driven work of transnational civil society and local, grassroots, movement-based organizing. These distinctions adhere to differing political commitments and degrees of institutionalization. For clarity, 'civil society' refers to a global field of transnationally coordinating digital security experts, technologists, and

Drawing on my findings from this study, the chapter provides an account of the imperative for affected communities to proactively act *on the time before* preemptively violent surveillance measures can exert harmful effects. This exploration of proactivity is intended to shed light on possibilities to challenge preemptive logics and anticipatory regimes. The chapter sits in dialogue with scholarly work on data justice, resistance to surveillance, and agency in a datafied society (Benjamin, 2019; Browne, 2015; Dencik, et al., 2019; Gangadharan, 2020; Milan and van der Velden, 2016; Van Dijk, 2014). Scholars studying these issues argue that what requires more attention is how different social groups can and do already intervene into the preemptive and predictive logics that suffuse contemporary surveillance and data-driven systems (Andrejevic et al. 2019; Gangadharan, 2020; Minocher and Randall (2020). The goal of this chapter is to contribute to this growing body of literature by exploring the preconditions and ambiguities of resistance to preemptive surveillance. 'Proactive' action is often framed as a future-focused orientation tied to a capacity for foresight and agency. In the context of policing, proactivity refers to data-driven preemption. In the context of activism, proactivity may refer to positive co-optations of data for social good, highlighted as examples of empowerment and agency. This chapter adds a new dimension to understandings of proactivity in relation to policing, activism, social movements, and civil society, re-contextualizing proactivity to mean an imperative to act before probable harm is caused by violently

NGOs involved in 'internet freedom' and digital rights, while the 'movements' at play are the grassroots community organizers and their constituent communities in Los Angeles, in the United States. In exploring efforts to resist and counter preemptive surveillance, the chapter explores the meeting points and divergences of civil society actors and movement based community organizers, noting both their common goals and differences.

preemptive actors. The chapter investigates how this form of proactivity is embodied and enacted when imbricated within the security/safety practices of human rights defence and social justice organizing work. The relationship between preemption and proactivity is explored through two cases drawn from ethnographic field work around transnational digital rights and Internet freedom communities that develop technical counter-measures for security and surveillance, and fight for different notions of justice and rights in relation to technology and society.

The plan of the chapter is as follows: in the next section, I contextualize my concern with proactivity and strategies to counter preemptive logics, drawing on literatures relating to policing, surveillance, and activism and social movements. Following, I discuss my methods and research positionality. Then I introduce the two empirical cases of the chapter, each serving to highlight the importance of proactivity in the context of resistance to preemption. The first case explores resilience as enacted through structured security protocols in the context of a digital security exercise conducted to prepare for preemptive office raids of human rights organizations by state actors. The second case looks deeper at the efforts of the SLSC to challenge the carceral logics and practices of predictive policing in Los Angeles through the collective refusal of abolitionist community organizing. The chapter concludes with a critical discussion of empowerment and agency vis a vis the imperative to act proactively against preemptive harms.

Preemption, proactivity, and empowerment

This chapter explores how preemptive logics are countered in two different settings. In both, the chapter identifies and explores an orientation towards proactivity and the seizure of the spatio-temporal 'not yet' as a locus point between violent state security apparatuses and social movements defending their autonomy and lives. Whereas the 'proactive', orientation of policing has been explored extensively in criminological and security literature, this chapter explores 'proactivity' within actions taken to resist, contest, or find safety amidst violent anticipatory regimes. This section of the chapter does two things: first, it provides a short overview of preemptive surveillance and policing and contextualizes proactivity in relation to literature. Second it looks at proactivity in relation to resistance to preemptive measures, community organizing, and contemporary activism.

In the context of surveillance, security and policing, preemption implies the will (and power) to forcefully intervene against undesired futures. In practice, the ability to act preemptively implies the use of violence to foreclose the futures of people deemed risky or undesirable to powerful institutions and actors (Andrejevic, 2020; Benjamin, 2019; Browne, 2015; Wang, 2018; Williams, 2019). Preemptive security and surveillance do not by definition imply the use of big data, nor are they 'new' phenomena (c.f. van Brakel, 2016). Preemptive actions such as raids, arrests have been a long-standing concern for social movements (Gillham, 2011; Porta et al., 2006). Further, preemption has been explored extensively as a political ideology driving counter-terrorist actions by states after 9/11 (Amoore, 2013; Anderson and Adey 2011; de Goede, 2008; 2009; 2014; Suchman, 2017; 2020). Dencik et al. (2015; 2018) and

Gillham (2011) highlight preemptive measures such as preemptive arrests, the disruption of protests through checkpoints and searches, and 'kettling' (Swain, 2013) in order 'to isolate and contain disruptive protesters whether actual or potential' (Gillham, 2011: 637, in Dencik et al., 2018). These kind of preemptive actions do not necessarily depend on the use of digital, big data-driven surveillance per se, however, the use of different forms of adversarial information collection and intelligence is essential, and can be understood as part of an unfolding history of 'Intelligence-Led Policing (ILP) (Browne, 2015; De Hert and Vis 2005; Van Brakel, 2016).

Per the SLSC (2018), ILP has 'oriented law enforcement towards activities of data gathering, data analysis, and preemptive action against presumed criminal and terrorist activity'(4). Scholars from across criminology, security studies and surveillance studies characterize intelligence-led policing as part of a shift from 'reactive' to 'proactive modes of action in policing, constituting a 'turn' to proactive modes of 'disciplinary power' (Andrejevic, 2020: 87). Broadly, the term 'proactive' in this context is used to characterize the intwining of data-driven techniques and future-oriented temporal logics (Bigo, 2006; Brayne, 2016; Dencik et al., 2017; Massumi, 2015). Per Dencik et al. (2017), the 'transformation from 'reactive' to 'proactive' policing combines data analysis with human intelligence and interpretation' (pp.1146). It is in this longer trajectory in 'proactive' punitive and violent state action that novel predictive policing techniques and platforms have been promoted and sold to police departments around the world. 'Big' data and data-driven policing platforms augment and propel the preemptive logics of ILP in new ways, entrenching a longer move towards quantitative and statistical methods of policing (Didier, 2018). Andrejevic et al. (2019) characterize the logic of predictive policing as a 'just-in-time' temporality premised on preempting an event just before it happens, 'so there is sufficient evidence to detain or arrest, but the crime itself is averted.'(3). This is a defining element of 'the compressed temporality of preemption, which simulates an anticipated future in the present so as to act upon it before it can occur' (Andrejevic, et al., 2019: 4) in order to 'optimize the precious time that police forces have'(Funnell, 2015 quoted in Andrejevic, 2020: 86).

In the section above, I contextualized the notion of 'proactivity' in relation to policing, a context in which proactivity is a violent, time-bound and data-driven orientation growing out from histories of racist oppression, carceral institutions, techniques of war, and an intensified surveillance society. Here I highlight that proactivity also arises as a theme in studies of contemporary activism, signifying a form of empowered use of data. 'Proactive data activism', as coined by Milan (2016) and further explored by Gutiérrez and Milan (2019) relates to efforts by 'data activists' to exploit the new availability of 'big data' in support of varied notions of social good. Data-intensive projects such as Ushahidi and other participatory mapping projects are explored as positive co-optations of dominant logics and potential portals to alternate imaginaries of datafication. Within this heuristic, proactive data activism is contrasted with 'reactive' data activism, which refers to efforts to resist surveillance and datafication, including through safety and security practices. Considering that this chapter's concern is with safety and security, the 'proactive' actions explored in this chapter do not neatly align with the data activist proactive/reactive heuristic. Rather than referring to the exploitation of available data towards 'positive' activist ends such as those described above, proactivity in this chapter refers to a temporal orientation which emerges within the imperative to urgently prevent or mitigate harms caused by the intersections of surveillance, carceral technologies and oppressive preemptive actions. That being said, I will later show that in the context of security practices, the ‘proactive’ orientation towards future harm can lend itself to data-driven action, as in the first case of this chapter, which explores civil society’s turn to data-driven resilience in security. In contrast, in the second case, proactively arises within the abolitionist refusal to engage with or be captured by data and its underpinning logics all-together. This tensions between resilience and refusal, and how the use of data figures into these two strategies, is explored in subsequent sections of the chapter. For now, I end this section of the chapter with a question. Having noted that proactivity comes into play for both violent, preemptive actors and, consequently, their subjects, it is worth asking to what degree proactivity always implies empowerment, and if it does, is this the kind of ‘empowerment’ that is invoked in the positive sense of the word with regards to ‘proactive data activism’? This is a question I return to later.

Methods and research positionality

This chapter draws on data from 50 interviews and participant observation field work conducted with NGO staff, human rights defenders, digital security specialists, and social justice organizers working with communities affected by surveillance between 2016 and 2019. The selection of interviewees resulted from purposeful sampling at 12 international meetings and conferences devoted to promoting Internet freedom, digital rights, digital justice, and social justice in Europe and Southeast Asia. Interviewees come from 26 countries, a result of the demographics of the gatherings where fieldwork was done, which are representative of the transnational nature of the larger field concerned with issues around human rights, social justice, and technology. This field is comprised of heterogenous communities with oft-conflicting politics (c.f. Mouffe, 2013; Horgan and Dourish, 2018), which nonetheless coalesce at international events to discuss common threats, shared values, and to establish consensus – where possible – on 'best practices' around digital security, digital rights, and related issues. This chapter draws on these interviews and participant observation for its analysis of proactivity, a theme discussed across the heterogeneous communities interviewed in my research. The two cases featured in this chapter highlight two particular contexts of human rights and social justice work, where the actors above contend with preemptive measures through different forms of resistance and contestation. The first context explored is an international training bringing together people from the human rights defender community from all over the world to develop security preparedness protocols. The second context concerns the work of STOPLAPD Spying Coalition, looking in particular at a conversation staged by the organization at a digital rights conference in Europe, where they about how to counter the harms of predictive policing. In this chapter, all interviewees and the groups they work with have been anonymized due to safety concerns. Certain organizational names remain, with their consent.

A note on my research positionality: inspiration for this chapter comes from my own background of practice in the field of digital security and safety for human rights and social justice, during which time I worked with different NGOs and grassroots groups to understand how to connect matters of safety and security to broader movement goals (Kazansky, 2015; 2016). Throughout my years engaging in this work, tactics and strategies employed towards the goal of safety underwent continued iteration and contestation amongst security practitioners and the groups they worked with to devise strategies for safety and security (as I document in Kazansky, 2021 and Kazansky and Milan, 2021). During my time as a digital security practitioner, I often encountered boundary conflicts around what constitutes effective 'individual' and 'collective' action as it pertains to self-defence and community defence; an observed disillusionment with technical 'solutions' to surveillance; increased efforts to grapple with racism, neo-coloniality, carceral logics, and diversity issues within the field itself, and the continued re-configuration of pedagogical practices to help groups imagine and prefigure just futures. As the issues highlighted above have made their mark on digital security practice within transnational civil society, digital security practitioners have reflected on how the practices they promote and teach can better support the goals of the grassroots groups and movements which they engage with. It is in this spirit of this weighty responsibility that I engage in this chapter with the unjust histories and practices of preemption and the vital contributions of abolitionist thinking and organizing to social justice, as it is now advanced by STOPLAPD Spying Coalition and other groups highlighted in the chapter.

The proactivity of *security preparedness protocols*

> "For people to make time for security is really difficult. Every day there are so many immediate threats that need to be handled and the work never stops unless someone is dead or

> has experienced some breakdown. People react to immediate threats and the challenge is to get them to think about long term planning, strategy, to have a policy in place before things happen, and to be proactive instead of reactive" (Interview #6).

This quote is from a digital security trainer who teaches security countermeasures to international human rights nonprofits and grassroots groups across different regions of the world. His repertoire as a trainer addresses a spectrum of technologically related security incidents of concern, from suspected computer compromise, to online harassment and defamation campaigns by state sponsored actors. As his experience indicates, the challenges of human rights work require making time for security before insecurity forecloses time. He emphasizes that human rights defenders must be 'proactive' lest they overtaken by harm. But what does it mean to be proactive in the context of security practices for human rights work? This was a central subject of discussion at an observed training taking place in 2018. This section of the chapter explores the site of this digital security training as a liminal space constructed to help those concerned with safety harness the 'tensed time-space where disaster is not-yet, action is demanded, decisions are weighted with consequence, and action is animated by necessity and urgency' (Anderson and Adey, 2011: 1102). The vignette in this section positions the training as a jumping-off point to explore how the security protocols are taught in order to mitigate potential harms of digital threats. As part of this exploration, I look at how these security protocols are productive of a particular regime of resilience and 'resilient subject' (O'Malley, (2010).

The training, staged in a quiet European city by a long-established human rights organization working at a transnational level, brought together a group of 20 self-described human rights defenders[24] (HRDs) from 16 countries to learn practical security countermeasures. A number of HRDs arrived seeking reprieve from urgent concerns, working with families of the desaparecidos in Mexico; with LGBTQIA+ activists in Nigeria; with digital rights organizations in Tunisia; and with women's rights activism in the Philippines[25]. Taking place over five days, the event comprised three educational modules divided into topics of security from a digital, physical, and 'psychosocial' perspective. On the table were everyday data issues affecting non-profit organizations and grassroots initiatives: digital device failure, data theft, commercial data exploitation, as well as concerns particular to human rights work: preemptive office raids by local police and national security agencies; targeted attacks on high-profile HRDs; the wiretapping and digital monitoring of movements' online activity and violence against women online and 'offline'.

After several days of software demonstrations of security counter-measures such as password management software and encrypted email, the participants were asked to synthesize 'learnings' through

24 The term 'human rights defender' is common to the international human rights community, used to describe and legitimize the work of individuals engaging in a number of different forms of activism. The status of human rights defenders as people and groups deserving protection has been legitimated through UN processes such as the United Nations Declaration of Human Rights Defenders (1998). See: http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Declaration.aspx and 'Who is a defender?': http://www.ohchr.org/EN/Issues/SRHRDefenders/Pages/Defender.aspx.

25 Names and other identifying details have been changed

engagement in a speculative scenario planning exercise. Sitting together in a circle, the trainer asked the group to imagine that an office raid was about to occur at a hypothetical non-profit civil society organization. Office raids have been well-documented in the international human rights community in recent years, with an observed increase tied in part to a string of new national security laws implicating human rights organizations as 'foreign agents' or actors in countries such as Russia and India (Amnesty International, 2017). As human rights organizations document, vague suspicions of foreign influence are invoked to justify a raid (Elder, 2013; Human Rights Watch, 2020). During a raid, police or security actors may grab paperwork, seize or destroy digital devices and threaten physical intimidation, justifying these actions on the suspicion that the civil society organization has broken the law tInformation exfiltrated through the raid is then used to build a legal case against the organization and used as grounds to shut down an organization's operations. To gather the greatest quantity of compromising or incriminating information requires catching the organization unprepared. Thus office raids must be planned to take place 'just in time'(c.f. Dencik et al. (2017) in order to maximize the element of surprise. The digital security trainer leading event observed that raids often follow on a period of digital or physical monitoring of organizational infrastructure to identify potential weaknesses and vulnerabilities in their work and technology. This kind of preemptive scanning of organizational vulnerabilities enables the party planning the raid to determine the best moment for the execution of preemptive action.

'An office raid is imminent. What should be done to prepare?' On a white board, the security trainer asks the participants to break down potential mitigations into two columns: 'reactive' and 'proactive'.

‘Reactive’ connotes actions taken in the immediate wake of an emergency event, digital or physical. ‘Proactive’ refers to preparations that could be made ahead of time in anticipation of probable threats. In the reactive column participants add suggestions such as ‘keeping calm’ ‘staying vigilant’ and ‘sending an SOS message to a colleague’. One participant notes a dilemma: amidst the urgency of an office raid, there might not be enough time to reach out to a colleague for help. Hence, it is deemed essential by the training participants to ‘know beforehand who to turn to if you need money or technical support’(field notes, 2018). If receiving assistance in the middle of an emergency requires time that’s not there for the taking, processes should be set in place beforehand in anticipation of problems, argues the trainer, as though, per Adams et al, (2009), ‘the event and the trauma...were already here’(257). When this emergency inevitably occurs, there will not be the time or space for deliberation to determine how to best respond. This implies that security and safety is only be possible if HRDs can match the ‘just in time’ tempo of preemptively threatening actors and perpetrators of violence through structured preparedness protocols.

The training participants thus discuss the need to put in place a spokesperson or ‘lifeline’ ahead of time in order to increase the chance of being able to contact them in the midst of the hypothetical emergency. In the proactive mitigation column, participants write: ‘select a spokesperson, have a lifeline, monitor the context, check the local law’. The digital security trainer of the training suggests that a proactive mitigation could also include the creation of data backups in anticipation of its loss (a practice highlighted by pink et al. (2018) as an example of an ‘anticipatory mode’ of data practice, which I further expand upon in Kazansky (2021). Added to the growing ‘proactive’ column are: the installation of CCTV cameras around the office, the duplication and back up of sensitive data at a separate location, regular software updates to patch software vulnerabilities, and the use of digital firewalls against unwanted digital intrusions into networks and computers.

This enumeration of proactive and reactive actions exposes a tension in the temporal scaffolding of proactivity. What, a participant asks, is the moment at which an action should be designated as proactive? For example, if an organization begins backing up its data following a cyberattack or office raid, does that make the back up a reactive or proactive measure? On the one hand, the measures are implemented in response to an event. On the other hand, the measures are intended to prevent or mitigate the effects of future events. Though the reactive and proactive have been delineated as dichotomous, the leveraging of past experiences to inform future-oriented action shows that proactivity piggybacks on reactivity. To put it differently, the logic of proactivity harnesses an individual or community's experience of past harm to 'prime' itself (Massumi, 2015) for potential future threats. As the discussion in the security training shows, To take back time for security (as encapsulated in the elusive 'before') means to optimize for efficiency and engage in a temporal dance constructed by powerful actors to elude perception by their targets.

Further, as made evident in the above discussion, to 'proactively' intervene into a preemptive event is tricky, and its prevention is not always deemed possible. Due to the continuous threat of temporal foreclosure through preemptive digital compromise or violence, the trainer stressed a need to act in a more structured and efficient mode; to 'build standard operational procedures for the daily of human rights work' (Interview #39). This raises the question: what happens to ‘the before’ when there is not a singular event to prepare for, but a spectrum of violent potentiality ‘not yet emerged’ (Dencik et al, 2018: 1435)? What sorts of commitments (and burdens) are created through such a ‘proactive’ agential dynamic? For the trainer, the seeming impossibility of stopping preemptive actions means that the focus of ‘proactive’ security-related actions is not on always preventing threats but on their mitigation and continued management. ‘Operational stuff needs to be structured as much as possible. This is what I mean by proactive’, the trainer further explains, highlighting the need for detailed, formalized plans for safe travel, for movement from home to office; for how to download suspicious documents form the Internet; and for how to behave online if targeted surveillance is suspected. Structure and formality are seen to bring efficiency to crisis response; to meet the challenge of a lack of time and space in the moment of preemptive violence.

This trainer’s approach is exemplary of a broader movement of ‘proactive’ action against digital security incidents within an increasingly formalized and specialized field. As of the writing of this chapter, an increasing number of transnational NGOs run hotlines, help desks, triage services, and information sharing platforms which document security incidents and mitigate their effects, encouraging human rights defenders and movement actors to reach out in event of crisis. Security specialists look for patterns in the nature and frequency of incidents, using this data to inform resource allocation and to secure infrastructures amidst anticipated disruption (Kazansky, forthcoming). The emphasis on structure, data, and continued vigilance result in a focus on resilience. A security specialist building out an information sharing platform argued that for her field, digital security has become about resilience ‘because shit is inevitably going to go wrong, and we want to enable our partners to be resilient to the impact of that when they do happen' (Interview #42).

The proactive security stance, as embodied through the paradigm of data-driven resilience, hinges on two assumptions: first, that future harm will occur, but, second, the harm can be mitigated by collecting and synthesizing data about these harms and future potential threats on a continuous basis. As with the turn from 'reactive' to 'proactive' policing, per McCue (2015), resilience, as imagined within the digital security practices of these transnational civil society actors, constitutes a 'shift from describing the past' (24) to an approach focused on continued, data-driven management of anticipated harm. Effectively, individuals and groups affected by surveillance and digital threats are required to continuously anticipate preemption, a mind-twisting and circular proposition. It should be noted that resilience is a highly contested term endemic to the language of security regimes, state institutions, and corporations (Bourbeau, 2018; Coaffee, 2013; O'Malley; 2010). Resilience is critiqued by critical scholars of criminology and security as a regime of care premised on managerial logics of individual responsibility, propelled by state actors who have reneged on their duties of care towards citizens. This is one conception of resilience. On the other hand, however, resilience implies survival. Discussing findings from research and community organizing around data justice in three US cities, Petty et al., of the Our Data Bodies Project (2018) underline that people facing continued insecurity – here 'Charlotteans, Detroiters, and Angelinos' – are 'resilient in spite of persistent and destructive forms of surveillance and profiling'(1). As such, resilience here is understood as a necessity amidst longer-term struggles for social change; necessary because bringing an end to unacceptable practices and institutions takes time. Nonetheless, it is one thing for a community to celebrate its own resilience and another thing for a violently negligent institution necessitate this resilience in the first place. In light of the ambivalence around the necessities and injustices of resilience, the question becomes how to attend to matters of every-day survival amidst probable future threats (in other words, to be resilient) while also moving towards a larger horizon of possible futures in which threats are not inevitable. This question is explored in the next case of the chapter.

The proactivity of *dismantling of harmful systems through abolitionist refusal*

The last case discussed tactics to counter preemptive logics in the context of office raids. I documented the efforts made by NGOs and human rights defenders to 'proactively' ready themselves for future raids on their organizations, and how this kind of tactical safety work is conducive to a strategic focus on 'resilience' in the face of probable future threats. In this section of the chapter, I turn to another field work context where preemptive logics were countered, coming back to the work of the StopLAPD Spying Collation (SLSC) introduced at the start of the chapter. The SLSC is a group of volunteers that proactively challenge the preemptive logics exerted by a police force against populations living in the city of Los Angeles. While the security training in the first case was concerned with how to take tactical action against a particular preemptive manoeuvrer, the SLSC's focus is on challenging preemptive logics – and their carceral underpinnings – at an 'ecological' level (StopLAPD Spying and Free Radicals, 2020). Rather than conceding to the inevitability of future threats and harms, the SLSC actively fights against their aura of inevitability through a focus on the abolition of the implicated systems and the re-imagining of just ones in their place. The vignette below introduces their work through an encounter at an international conference on digital rights and digital security. It then highlights how 'proactivity' is key to SLSC's fight against preemptive injustices, while also surfacing tensions between the different ways that transnational digital security specialists and grassroots community organisers contest surveillance and data related injustices.

In 2019, volunteer members of the SLSC traveled to Europe to give a presentation at an annual conference on Internet freedom and digital rights. In their presentation, they expounded an urgent case for why an abolitionist approach is necessary in order for movements to successfully tackle technologically related injustices, showcasing their work to dismantle predictive policing programmes in Los Angeles. The audience was largely comprised of nonprofit workers, tech activists, and digital security trainers from around the world. What united many of the audience members was their investment into the promotion of Internet freedom tools and digital security countermeasures such as encrypted email clients, VPNs and secure messaging applications. Making introductions at the front of the room, one SLSC volunteer began their presentation with a provocation: predictive policing, they said, 'isn't something we are going to solve with an encryption training' (field notes, 2019). With this statement, SLSC aimed to disrupt the audience's focus on technical mitigations for surveillance harms and data injustices. The presentation introduced the coalition's working principles and research, including their abolitionist analysis of the 'architecture of surveillance'(SLSC, 2015) and the 'ecological' configurations of unjust algorithmic systems and their intwining with institutional racism (StopLAPD Spying and Free Radicals, 2020).

Throughout the presentation, the coalition emphasized the systemic nature of harm; arguing that the harms are not accidental but intentional, and that they did not just take place in ‘a moment in time’, but throughout a long history of injustice (field notes, 2019). Nor is the problem of predictive policing simply a matter of an unruly algorithm or ‘dirty data’ that can be fixed through technical ‘de-biasing’, they argued. The coalition’s philosophy and working principles were not self-evident to at least some members of the audience, as became clear in the question and answer period that came at the end of the presentation. One member of the audience asked the coalition if they might consider training those affected by predictive policing harms in Los Angeles to use a secure computing system for their daily communications. A second asked: couldn’t making policing more community-centric be a way forward? The SLSC provided the audience with emphatic answers for why these suggested actions are not a part of their repertoire. Regarding the suggestion to conduct digital security trainings on ‘secure’ tools, the SLCS reiterated that like any other group concerned with surveillance issues, everyday safety is a concern. However, the larger aim of their work is not to promote self-defensive digital security practice. In fact, the organization de-centres what they view as an unhelpful focus on technology and so-called tech-‘fixes’. Rather, their work focuses on the dismantlement of the broader systems generative of surveillant and carceral logics and technologies. Coming back to the SLCS report introduced at the start of this chapter, the interviewed volunteer explained that:

> that’s the biggest point of the phrase before the bullet hits the body. The focus is on structures. This isn’t about

> just changing a programme or becoming more community oriented. The concern is not the bad apple. It's the system that is rotten at the core. It has to go completely (Interview #43).

The demand for the systemic dismantling of the racist, carceral 'stalker state' and its manifestations within 'smart' policing mechanisms is at the heart of SLCS's abolitionist approach to community organizing and policy change. In their community outreach strategy and in the awareness sessions they facilitate they are is focused on 'realizing there are programs, systems, structures that can essentially be ended and can be dismantled' (Interview #43). SLCS's work is part of a growing movement of grassroots initiatives engaged in abolitionist work that connects the ongoing fight against racism and carceral systems with technological injustices emerging in an era of datafication and ubiquitous digital surveillance (c.f. Benjamin, 2019; Datafication and Community Activism workshop, 2019; Emmer et al,. 2020; Gargandaran, 2020; Miller, 2019; Milner, 2019; STOPLAPD Spying Coalition 2018; 2020; Wang, 2018). This movement includes organisations such as the Carceral Tech Resistance Network[26], Critical Resistance[27], and Data for Black Lives[28].

Having introduced the stakes of SLCS' fight against the inevitability of harm, this section of the chapter explores how the time-space before preemptive violence figures into the abolitionist approach exemplified in SLCS's work. How to characterize the temporal dimensions of abolition in relation to the 'not-yet'? One answer is

26 https://www.carceraltech/

27 http://criticalresistance.org

28 https://d4bl.org

that abolition is about friction and slowness, as per Sarah T. Hamid of the Carceral Tech Resistance Network, who writes of her abolitionist work on technology that unlike the ‘frictionless innovation’ pushed by Silicon valley culture, ‘you have to live in the friction. You have to be slow’ (Hamid, 2020). Following Hamid’s conceptualization of abolition, to refuse or to call for the dismantlement of something would imply a stoppage or slowing down of action. Slowness is also proposed as a counter to preemptive actions by Andrejevic et al., (2020) who critique preemption as a manifestation of accelerationist logics under high capitalism. Yet, the SLSC volunteer who I spoke to makes clear that if abolition is about friction and slowness, it is also about urgent action, explaining that ‘we use the abolitionist framework because we don’t want to lose time. Because we are losing people’ (Interview, #43). This is to say that the urgency for the work of SLSC to shift from ‘reactive’ to ‘proactive’ action – in other words, to urgently grab back time, space and possibility – resonates with the urgency of the digital security trainer and human rights defenders in the preparedness training featured in the prior vignette. Describing the move to a proactive orientation, the interviewed SLSC volunteer explained: ‘we were always in response mode. Something happened; someone died’. Eventually the organization began:

> moving away from just reacting but acting before everything happens...staying ahead of the game, pacing ourselves and are not just on being on the receiving end. Stopping it before it leads to someone’s death. I go back to talking about the things we need to do before we die, things before we are murdered by the state; things to do before we are incarcerated (Interview #43).

In light of the urgency with which SLSC works, I return here to the question and answer period of the conference discussion held at the digital rights and Internet freedom conference. Following the first question about digital security, another audience member earnestly asked if SLSC had found an opportunity to sit down in dialogue with the police force in order to help them understand the harms of their actions to the community and aid them in reforming how it conducts its activities. For the SLSC, the invocation of community stakeholder participation as a solution to carceral harm tracks with an over-emphasis within civil society on the notion that harmful technologies can always be 'reformed'. 'You can't reform something based on such shaky grounds', the SLSC volunteer underlined for the audience. 'Sometimes reform leads to complicity in atrocities', he further argued, especially since the harms perpetrated by the police were not an isolated mistake, but rather, 'the harm is the point'. In light of this intentional harm, the volunteer asked the audience back, 'why take a seat at the table' in discussion? (field notes, 2019). Indeed, the SLSC provides a direct affront to the idea that policing – even where reframed as community driven, participatory, or democratic – is redeemable as an institution (which Gangadharan, 2020 characterises as a form of organized, community-level refusal). Where reformist policing initiatives strive for incremental change through existing institutional arrangements and small regulatory fixes, 'we don't want to waste time on legislation that will just blunt the edge of a knife, because a blunt knife is more painful.' (Interview #43).

Towards the goal of abolition rather than reform, the SLSC has engaged in a number of actions, making public records requests to learn more about policing programs and filing a Public Records lawsuit when they proved unresponsive (SLSC, 2019a; SLSC, 2019b); providing testimonies of police violence and community harm at public sessions; running community education seminars and teach-ins to map and directly challenge claims made by the police in public debates held at Board of Los Angeles Police Commissioners (BOPC) meetings, among other activities. It was their vocal demands at these meetings (spurred on also by the research featured in the report 'Before the Bullet Hits the Body) that lead the BOPC to hold a public hearing on Operation LASER in 2018. This public hearing resulted in the audit of the Strategic Extraction and Restoration (LASER) Program, to which the SLSC responded with further critique (SLSC, 2019b).

Around the time of our interview in 2019, SLSC was celebrating the end of the LASER program, bringing with it the end of the chronic offender bulletin, a risk scoring system which had disproportionally targeted the Black community (Puente, 2019). The SLSC attributes its end to the multi-year campaign it waged against it. At the time of its announcement, however, the police chief emphasized a continued faith in data-driven strategies of policing (Baek and Mooney, 2020). Hence, another goal of SLSC was the dismantlement of one of the other main predictive policing programmes, PredPol, a 'hot spot' based predictive policing program which broke the city of Los Angeles into 500-by-500 square foot blocks. Following another year of organising, its discontinuation was announced on April 21 2020. In a chapter covering the LAPD's decision in the LA times, the decision was attributed by Chief of Police Moore to economic reasons; 'the cost projections of hundreds of thousands of dollars' (Miller, 2020) – though public push-back by groups such as the SLSC had clearly caused it to lose its lustre. Whatever the reason given, the chief reiterated a belief in 'the underlying principles behind Pred-Pol' as 'valid' and pointed to a newly revised strategy that would take its place, which he called ‘data-informed community policing’. This newest iteration of intelligence-led policing only served to confirm SLCS’ distrust in the notion of ‘community participation’ in policing as a viable way forward towards rectifying injustices. Here,‘community’ had been weaponized within the evolution of predictive policing towards further policing programmes and injustices. Hence, despite the end of the above programs, SLSC has had to remain ‘proactive’; vigilant about the rebranding of predictive policing under new names, covers, and rationales. The volunteered SLSC interviewee acknowledged the continuation of the fight: ‘we are staying ahead of the game and are pacing ourselves and we are not just on the receiving end...all of this is still a work in progress’(Interview #43).

Tensions between resilience and refusal?

Having considered the SLSC’s abolitionist work to counter preemptive logics, I find it important to ask how the resilience strategy exemplified in the first case, and the abolitionist refusal discussed in the second case, sit in relation to one another as respective approaches to countering the harms of preemption. First, I underline once more that these two approaches both involve the embracing of a notion of a future-oriented ‘proactivity’ in response to harm. Yet this proactive orientation is imbricated differently in the two counter-preemptive contexts discussed in this chapter. Though I do not place the two cases or the approaches which they discuss in direct comparison with one another, my concern is with a potential tension in how these two respective approaches prefigure the relationship of groups and individuals to desirable and undesirable futures. I point to the fact that for the group of human rights defenders and the digital security trainer featured in the first case, their proactive orientation was bound to the assumption that preemptive threats will continue to materialize in the future. The programme of resilience promoted by digital security actors in this case proffered a way to 'live' with or manage these continued, inevitable threats – but did not necessarily concern itself with a vision for how to tear out the roots of its source. Instead, resilience was elevated from a necessary, every-day tactic of survival to an overarching strategy and programme for data-driven action amidst assumed future threats. In contrast, the SLSC's work is explicitly orientated towards bringing an end to the source of the threat by dismantling the threatening ecology of technologies, institutions, and actors. Their abolitionist approach implies another orientation towards the future and its possibilities – one that is prefigured around a radical re-imagining of existing institutions and practices.

I underline that despite this tension arising around futurity and inevitability, the approaches taken in this chapter's two cases to counter preemption are certainly not mutually exclusive. Indeed, within the tactical dimensions of daily practice, efficient, structured security protocols may be applied towards the end goals of both resilience and abolition. Further, every-day resilience tactics are inherent to community centred work to counter the harms of data, per Petty et al., (2018) and Lewis et al., (2018: 38). Furthermore, as the participants of a community-centred workshop on activism taking place at UC Irvine (Datafication and Community Activism Workshop, 2019) underline, abolition work can – and should – allow for divergence and multiplicity in strategy, and do not necessarily imply the rejection of technological practices altogether. For example, Milner (2019) highlights that abolitionist work involves making use of data and data-driven techniques towards anti-racist goals, a goal pursued by her organization Data for Black Lives. This confirms that, as I have also argued elsewhere (Kazansky, 2021; Kazansky and Milan, 2021) resisting surveillance and its harms often involves both co-opting and re-configuring its logics through the creative intwining of tools, tactics, and strategies from disparate realms. Hence, I argue that the tension in how resilience and refusal prefigure the future can be understood as part and parcel with the ambiguity that accompanies living with surveillance and injustice while also fighting for its end. Yet the potential for resilience strategies to reify resignation to inevitable future harm leads me to ask if there are there instances where the managerial, resilience-driven approaches to security arising in the context of transnational NGOs and security specialists might be more closely aligned with the abolition-centred work of grassroots community organizers. To ask this question more normatively, are there ethico-political considerations particular to civil society digital security practice which might suggest that resilience should be de-emphasized as the overarching strategy guiding this work? This I leave as a critical question for further future discussion.

Between resilience and refusal: concluding thoughts

In this chapter, I have shown that for communities affected by preemptive and data-driven policing measures, acting on the space-time of the 'before' or 'not-yet' implies finding ways to interrupt the ability for a small group of powerful actors to determine who deserves to live. But how? Drawing on the prevalently expressed need amongst people interviewed in my study to 'act proactively' in pursuit of safety in situations where preemptive threats loom over their work, I argue that proactivity can be understood as a precondition for counter-acting the preemptive, surveillant logics of violent state actors. Through the study of two cases of resistance to preemption, the chapter has shown that for communities affected by surveillance, to proactively act on the time before preemptive measures are enacted can imply a number of different paths of action. The chapter explored 'proactivity's as it arose within two contextual strategies of counter-preemption. The first case looked at how an imperative to act proactively arose in the context of digital security preparedness. I showed that for digital security actors striving for efficiency of digital security in response to emergencies, the proactive orientation involved creating structured protocols for behaviour in dangerous circumstances, and has lead security specialists to embrace the use of data to more efficiently anticipate and recover from future threats. I showed how this proactive orientation towards the future culminated in a programme of data-driven resilience focused on the management and mitigation of assumed future harm.

Second, I explored abolitionist refusal as a strategy of proactive counter-action, looking at how abolitionist community organizing has contributed to bringing an end to the preemptive threats of carceral, data-driven systems of surveillance, in the particular context of predictive policing in Los Angeles and the work of STOPLAPD Spying. I looked at how STOPLAPD Spying challenged the inevitability of future surveillance and related threats through a refusal to take a seat at the table with harmful actors and by refuting the idea that reform can be achieved within an unjust system. In the end, I argue that the proactive orientation towards future harm, as discussed by interviewees and imbricated in their work to counter preemption, exemplifies the many ambiguities which accompany efforts to resist the hegemonic, ‘anticipatory regimes’ of contemporary surveillance (c.f. Amoore, 2013; Andrejevic et al. 2019 Mackenzie, 2013). While the ability by people put in harm’s way to act proactively is exemplary of their agency and counter-power; the fact that they must do so highlights the extent of injustice that different groups and communities face. One could say that in the same way that resilience arises by necessity – so does proactivity, and in the same way that resilience is weaponized by institutions reneging on their duties of care, so does proactivity arise in the absence of protection from above. As such, I argue that those who study activism and movements should take care not to reify ‘proactive’ forms of action as an unproblematically positive phenomena in a datafied society, but to contextualize it instead as necessity by virtue of violence and injustice. Having made this argument, it is my hope that this exploration of proactivity can contribute to the interdisciplinary imperative espoused by critical scholars of data and automated systems to demonstrate that harmful technologies and institutions do not stand uncontested; nor are surveillance and harm inevitable facts of social life in a datafied society.

CHAPTER 9: CONCLUSIONS

Overview of thesis

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

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

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

The anticipatory dimensions of resistance to surveillance emerged as a central theme in my analysis. I showed that making sense of the threats of surveillance and datafication involves future-oriented, anticipatory practices, which help transform unwieldy surveillance uncertainties into manageable contingencies. These anticipatory practices emerge from a widely expressed imperative to proactively avoid or mitigate the harms of undesirable futures. I thus used anticipation as an analytic through which to understand the temporal, affective, and political dimensions of living with and contesting a wide variety of potential threats. In my exploration of the practices and infrastructures particular to civil society's responses to surveillance, I have looked at how, to defend against surveillance threats, civil society actors appropriate anticipatory logics and practices from fields such as finance, state and corporate cybersecurity, and humanitarian operations. At the same time, I have also shown how civil society actors reconfigure different forms of anticipatory risk logics to reflect human rights and social justice. The next section of my conclusion gives a more detailed summary about the findings, theoretical contributions, and empirical contributions of the five core chapters.

Overview of findings in Chapters 4–8

In Chapter 4, I introduced my approach to studying the anticipatory dimensions of resistance to contemporary surveillance. In this chapter, I explored the anticipatory dimensions of two practices: threat modelling and risk assessment. I looked at how these practices are explicitly structured to guide action amidst surveillance uncertainties. I investigated how they allow civil society actors to weigh the likelihood of imagined potential future data harms, articulate situational contingencies, and map these contingencies to appropriate counteractions. I looked at how they thus function as a heuristic aid for choosing practices and 'tools' to counter concerns about surveillance and datafication. My **contribution** with this chapter was to unite critical data studies literature on data practices with the study of risk and anticipation through a novel concept. This approach drew attention to the future-oriented dimensions of practices that counter and mitigate the threats and harms of contemporary surveillance. I did so through my proposal of the term **‘anticipatory data practices’**, which I use to describe practices such as threat modelling and risk assessment. I conceived of anticipatory data practices as a hybrid concept that brings literature on the politics of risk and threat construction into conversation with studies of everyday technology use. To accomplish this synthesis, I connected Anderson (2007; 2010) and Alvial-Palacino’s (2016) notions of ‘anticipatory practices’ with ‘data practices’ (as conceived in critical data studies) in order to describe practices which grapple with ‘data mess’ through anticipatory modes (c.f. Pink et al., 2018). Through this exploration of anticipatory data practices, I also sought to contribute to critical security studies literatures concerned with preemption and anticipatory regimes by showing how anticipatory logics are appropriated and reconfigured by civil society actors working beyond the State and the corporation.

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

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

In **Chapter 5,** co-authored with Stefania Milan, we introduced the notion of algorithmic **'counter-imaginaries'** to discuss how dominant commercial and state imaginaries of datafication are contested by civil society. Together, we addressed the emergence of counter-imaginaries within civil society's commitment to oppose dominant imaginaries of datafication as constructed by state and corporate interests. We also **constructed a heuristic** to help conceptualize how and why civil society actors have shifted their approaches to mitigating threats and contesting technological harms over the years. This heuristic broke down civil society responses to the threats of surveillance into three categories: stabilized, formative, and speculative. These categories describe the degree to which civil society actors have tamed and domesticated problems relating to digital security, privacy, and safety through particular technical 'solutions'. Constructing this heuristic was a way for us to tackle a question central to the larger, collaborative DATACTIVE ERC project, which was: **how do techniques and strategies of surveillance resistance shift in response to datafication?** In thinking through this heuristic, we sought to capture moments of disjuncture in civil society repertoires for addressing surveillance and data concerns. We understood these moments, during which particular problems and 'solutions' to the harms of surveillance and datafication collapse in relation to new threats and priorities, as leading to a change in resistant practices. To explore this change dynamic, we conducted three case studies of software projects. The first case dealt with new computing systems meant to mitigate the sophisticated security intrusions of state actors; a second case sought to intervene into the data exploitation that comes with Internet of Things networks; and a third case tried to prevent human faces from being turned into templates for widespread 'smart' facial recognition. These cases drew from data I collected for my thesis, as well as a focus group that Milan led with the developers of Dowse, one of the three featured projects.

We then identified how these three projects embodied the algorithmic counter-imaginaries of compartmentalization, awareness, and obfuscation. First, we explored the possibilities and limits of compartmentalisation as a software strategy and user practice operationalised by QubesOS. We showed that, on one hand, isolating different parts of a computing system (and computing practices) could help create 'safer' spaces for computing, in line with digital security priorities common to hackers and technologists. However, we also demonstrated that, in the practice and perspective of the software's users, it did little to guard against the corporate exploitation of data. Next, we investigated Dowse, an intervention into consumer IoT technologies. Here, we explored how technologists and security specialists draw on the ambivalent promise of 'awareness' in order to increase knowledge of threats. Our third case examined the use of CV Dazzle face paint by a group of human rights defenders and advocates concerned with the threats of facial recognition. We explored how CV Dazzle embodies the counter-imaginary of obfuscation as a way to sabotage data-driven biometric surveillances. Here, we again showed that the concept and practice of obfuscation provides a path of possibility beyond the capture of a particular form of surveillance, at the same time that its tactical utility remains quite limited and fragile. In summary, we drew on this data to challenge the way that dominant imaginaries of datafication configure users as 'either co-producers of surveillance or its helpless victims'(104)

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

As I described, the process of qualculative convergence unfolds across three stages: first, a digital security trainer establishes shared definitions of security and technology. Second, the trainer elicits stories about threats and concerns to synthesize the experiences of the group of people they are working with into a legible notion of risk. In this particular training, this process of synthesis occurs with the use of a risk matrix – a visual risk analysis tool that organizes and mitigates the vulnerabilities of daily life by different degrees of severity, impact, and degree of possibility. In the third stage, particular security mitigations are chosen and plans are made to implement them beyond the training space. The goal is to come out of such a training with a repertoire of strategies and tactics to mitigate the harms of digital threats, so that 'at the end of [the training] the individual can act' (Interview #12). In the chapter, I argued that my concept is a necessary intervention into rationalist discourses of security risk as a naturalized, pre-existing thing in the world – a discourse prevalent in commercial cybersecurity and enterprise risk management. In making this argument, I further a goal of this thesis: to de-centre state and corporate discourse about risk and security.

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

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

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

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

Summary of theoretical and empirical contributions

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

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

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

I have thus argued that more research is needed that explores how different social groups respond to the anticipatory logics that characterize contemporary life with technology. In doing so, I have taken inspiration from Adrien Mackenzie's work on the anticipatory work of machine learners (2013; 2017) and Sarah Pink and co-authors' exploration of the 'anticipatory modes' bound up in banal data practices (2018). Like MacKenzie and Pink, I bring my focus of anticipation to the daily politics of practices and infrastructures engaging with data. However, unlike these two scholars, my research particularly concerns the activities of civil society. As I argue, if contemporary life is now characterized by the encroachment of anticipatory regimes (c.f. Adams et al., 2009), it follows that it is essential to ask how anticipatory logics suffuse and shape the lived experiences and actions of citizens, targeted groups, and groups that strive to advance human rights and social justice. In this thesis, I have advanced this area of questioning by investigating the refraction of anticipatory logics as they move from state and corporate realms into the realm of civil society, and back through practices that appropriate and reconfigure anticipatory logics. My contribution to this discussion is to advance anticipation into the study of civil society practices that seek to counter surveillance harms.

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

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

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

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

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

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

As I have come to the end of my time working on my thesis, I have enjoyed the opportunity to discuss my findings with several generations of academics and security experts focused on the study and practice of technology and security. Through these discussions, I have learned that my research findings are highly relevant to a new field of security studies emerging from two decades of technical usability work, seeking to understand the 'human' dimensions of security (Adams and Sasse, 1999; Whitten and Tygar, 2005). Situated at the crossroads of computer science, cognitive science, psychology, and international relations, this emerging field organizes its concerns around the notion of 'socio-technical security' (Ferreira et al., 2014; Kroeze, 2017; Mujinga, Eloff, National Cyber Security Centre, 2020). Since 2014, socio-technical security has been actively developed in the US and the UK at academic and policy-oriented institutions concerned with cybersecurity, critical infrastructures, and national security. The field works from the relatively newfound acknowledgement within technical security disciplines that there is no simple separation between ‘technical’ and ‘social’ issues. Socio-technical security tries to flip the longstanding computer security trope that ‘humans are the weakest link’ in the so-called security chain (Schweitzer, 2003). It recognises that, in light of continued human failure to perfectly configure security technologies, it is the systems that must be changed, rather than the people. This is quite an important step within a field long dominated by a limited understanding of the inextricable sociality of technical practice and infrastructure.

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

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

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

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

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

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

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

The reading group meeting was organised by a group of academics studying security from a critical, interdisciplinary perspective. One of my respondents was a policy-focused scholar who expressed concern that my article was too enthusiastic about security risk management tactics and strategies in the context of pushback to surveillance harms. The scholar argued that individualized practices of risk management have inherently limited potential to solve the structural and institutional issues that produce the harms of concern. I responded to the scholar that I am in deep agreement with their view on the limits of risk management and related self-defensive actions as avenues for contending with ‘structural’ harms. Indeed, my thesis takes a critical perspective on individualized responsibility, as embodied in many practices concerned with security and risk management. Across the core chapters of this thesis, I show that while risk management strategies can serve to 'tame' certain problems and make them feel more manageable, there is a world of difference between managing or mitigating risk, and doing away with its source. One of the concerning aspects I observe with regards to anticipatory practices such as risk assessment and threat modelling in the context of civil society work is how they arise from a responsibility born by targeted communities to maintain continuous awareness of potential surveillance threats. I thus investigate how future-oriented thinking focused on risks and threats can intersect with (and even augment) violent master narratives about technology and innovation.

I believe the confusion about my positionality towards risk management might stem from the thin line I have toed with my thesis. I have worked to simultaneously show why certain practices become necessary, while also pointing to their frictions, disjunctions, and capture into hegemonic regimes of security, risk, and anticipation. Just as my thesis raises the above critical concerns with anticipation and risk, I also show that thinking and doing through the lens of risk remains deeply useful and even necessary, and that it can be quite difficult to move beyond it. In this regard, I argue that it is important to remember why the people interviewed for this thesis turned to risk assessment and threat modelling practices in the first place. This point was best articulated by a respondent featured in Chapter 4, who works both as a policy advocate fighting to regulate biometric technologies, and as a digital security trainer teaching individualized tactics of self-defense, including threat modelling and risk assessment. When I asked her whether she sees one mode of work more necessary than the other, she responded simply, ‘we need all the tools’ (Interview #41).

This advocate and trainer further argued that it would be an arbitrary exercise to try to make a hierarchy of usefulness around different tactics and strategies (such as between individualized tactics of risk assessment she teaches in digital security trainings, and the advocacy she engages with around high-level policy arenas). She noted that in her work across Central America, there were times and places where a particular form of intervention in technological threats and harms suddenly became impossible to actualize due to the surrounding sociopolitical and technical context. When this happened, she found it necessary to ‘reach into the toolbox’ (Interview #41) and draw on a tactic or strategy that would fit local constraints. In some cases, this adaptation meant doubling down on daily safety and security practices. In other cases, her focus became to advocate for a particular law or policy. Her explanation, in turn, reminds me of a long-time human rights advocate who I had the honor to informally correspond with over the years I worked on my thesis. This human rights advocate has devoted most of her career to providing practical lifesaving support to a small group of human rights defenders living within an increasingly isolated and totalitarian regime. Her support includes provisioning custom technical mitigations for continuously shifting information controls, and providing emergency legal when people are arrested. She told me that over the years, she has regularly been asked by funders why it is worthwhile to continue devoting funds to a form of work that doesn’t seem to ‘scale’ beyond the small groups she works with. She likes to remind those who will listen that ‘whoever saves one life saves an entire world’, quoting Talmud Sanhedrin 4:5. From her vantage point, it seems that while broader fights are fought, it remains necessary to attend to individual lives and the banal nuts and bolts that make the continuation of their fights possible. I believe the experiences of these two people demonstrate that there is no either/or when it comes to exploring paths beyond our current predicaments with technological harms. There is simply no clear line of separation between day-to-day practice and fights for structural change. The more we strive to understand their interrelations, the better we can imagine emancipatory avenues for engagement with technology.

I acknowledge that the ambivalent picture I present of resistance and risk may not be satisfying for those seeking to measure and compare different strategies of resistance to surveillance and technological harms. Yet, important truths are found in exploring this ambivalence (c.f. Eubanks, 2011). Over the course of my work on this thesis, I have reflected on my own ambivalent relationship with risk management, and my absorption into various forms of anticipatory regimes. Despite my intellectual interests in critiquing risk, explicitly risk-centric language and risk assessment has become an increasingly important tool in my life, especially since the start of the COVID-19 pandemic, which coincided with the final stages of writing. I belong to a cohort of people billions strong that is deemed by certain risk rubrics to potentially be ‘at risk’ of serious COVID disease. Every day since mid-February 2020, I have reflected with ambivalence on my position as someone so labeled and absorbed into a particular regime of risk-based governance and anticipation. The anticipatory regime at play for me in the context of this pandemic is a self-constructed one. It involves little automation, and there is no single disciplinary overseer managing my every move. However, it is an anticipatory regime I have been responsibilised into, in order to cope with my everyday safety concerns in the absence of much protection from above. This anticipatory regime rests on my ability to rapidly adjust my safety strategies amidst scientific uncertainty and confusing public health messaging, and also hinges on my reluctant consent to be labeled an 'at risk' person, one I have consented to because it has promised to afford me certain kinds of care from the public health system of the country where I reside. Unfortunately, the experience of many shows that the designation of broad swaths of the population as being 'at risk' serves to justify the austerity logics and necropolitical agendas, while care remains elusive. As a result, I am not satisfied with carrying this risk label. Still, if you ask me how this pandemic has treated me, I will probably preface my response by noting that I am at risk, which speaks to my ambivalent absorption into ways of doing and being that I find problematic.

Drawing on this personal reflection, I think it is important to remember that many of the people I have interviewed for my thesis have come to use risk assessment strategies in situations where they have been made responsible for their own protection. As I have argued throughout this thesis, methodologies of risk assessment and threat modelling provide a way to tame the uncertainties of contemporary surveillance and to establish concrete heuristics for action taken in the name of safety, when safety is not forthcoming from states or corporations. That people now embrace such tools as risk assessment and threat modelling can be understood partly as the result of a failure in duty of care at a state level. Going further, the embrace of these practices can also be understood as a direct result of active state spying and intrusion into civil society work. For this reason, I cannot negate the importance of risk management in the daily practices of people trying to strive for social change for the same reason I cannot negate the usefulness of being able to call myself 'at risk' in the middle of a pandemic. I believe that the importance of risk management and tactics that tame uncertainty must be acknowledged as having a place in a larger politics of data. At the same time, I believe it is the responsibility of people charged with spreading awareness about technological concerns and working with communities to mitigate threats and be mindful of the problematics of risk and anticipation. This is especially the case because risk assessment and threat modelling often continue to be expert-led activities. As I show in Chapter 4, the experts teaching these methods play an important part in enrolling people into anticipatory logics, a process that creates new commitments and responsibilities. Considering the crucial concerns I have highlighted regarding risk and anticipation, I think it behooves such people (myself included) to also explore how we might be able to move beyond risk.

Over the years that I have documented shifts in civil society and its threats of concern, I have observed that the problematics of risk and the hegemony of risk regimes have become a central area of contestation in local and international discussions about the governance of artificial intelligence systems and their harms. Community organizers and activists fighting against the harms of carceral systems explicitly draw links between institutional approaches to risk management and individual lives framed as 'risky' and 'at risk', critiquing the use of automated risk assessment strategies within data-driven policing and in the judicial realm. Arguing that it is not acceptable for our institutions to make risk subjects out of Black communities in the United States, Data for Black Lives Founder and Executive Director Yeshimabeit Milner asks: 'how did the word risk – which finds its origins in finance and insurance, become a label for people like me and my friends?' (Milner, 2019). The growing recognition of the hegemony and harms of risk-centric thinking and systems, I believe, is why the vital and long-standing work of abolitionist, anti-racist organizations such as Data for Black Lives have received increased amounts of attention in public debate and in academia. Now, community organizers argue that it is essential for this wider attention to be channelled towards co-liberation. This leads me to ask: what is my small part in this broader conversation? For my part, I argue that even as we continue to frame our lives through future-oriented logics such as risk, we should find ways to intervene in the hegemonic risk logics and risk rubrics that our lives are fitted into. But how? Per Amsler and Facer (2017):

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

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

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

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

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

I argue that the intervention my colleague and I made can be understood as a small-scale corollary to a current fight playing out in the European technology policy space. On the heels of seemingly unending crises of accountability surrounding big tech companies and artificial intelligence, as of July, 2021 the European Union (EU) is going through the process of adopting a new framework to help it better deal with the threats and harms of artificial intelligence. This new framework is premised on a risk heuristic that breaks down artificial intelligence systems into levels of concern from 'unacceptable' to 'minimal risk'. Drawn as a pyramid, the 'unacceptable' domain for AI use is the smallest – representing the tip of the pyramid – and is designated as the part of the pyramid where new regulation is most necessary. Meanwhile, the 'minimal risk' domain is the largest on the pyramid. The implication is that most AI risks can be countered through self-regulation. In response to this proposal, civil society organizations have spent the better part of 2020 and into 2021 arguing against risk-centric conceptualisations of AI harms. Digital rights civil society organizations such as Access Now call this risk framework an arbitrary exercise that gives too much room for self-regulation to potentially harmful systems. They also believe it ignores how data exploitation and automated systems can have existentially serious impacts even across 'minimal risk' domains of AI use. To counter the EU risk framework, civil society organizations instead call for the establishment of human rights-based 'red lines' approach to guide acceptable and unacceptable AI use. The idea is to draw clear lines beyond which any AI system with clear human rights impacts should be banned, rather than simply tamed through regulation. I believe the push by civil society organisations for a rights-based approach to AI regulation is a crucial intervention, and I see it as a high-level corollary to what my colleague and I tried to do on a very small scale with individuals and organisations concerned with their digital security.

By sharing these examples, I highlight that there are many ways to disrupt risk, whether by experimenting with risk language substitutes in digital security trainings, calling for red lines instead of risk rubrics in high-level policy fora, or pushing for the dismantlement of risk-centric carceral systems. Engaging critically with issues of risk at these different scales is a way to work towards 'enlarge(ing) the space of possibility' (Amsler and Facer, 2017) for more just futures. By challenging how institutions and communities construct risk, we can find ways to refuse and interrupt the anticipatory surveillance regimes that we live within. Further, by finding strategies to challenge risk- and future-oriented logics, we can also challenge deterministic narratives about people and technological systems. This, in turn, has the potential to make our technological systems and societal institutions better able to hold space for indeterminacy, substantively grapple with the root causes of uncertainty; and engage with the world in more just ways. In the words of anthropologist Anna Tsing, 'indeterminacy, the unplanned nature of time, is frightening...but thinking through precarity makes it evident that indeterminacy also makes life possible' (2015:34).

METHODS ANNEX

1. Interviewees

Interview #1: FLOSS volunteer technologist, conducted at a Hacker conference between 2016-2019

Interview #2: FLOSS volunteer technologist, conducted at a Hacker conference between 2016-2019

Interview #3: commercial & nonprofit cybersecurity specialist, conducted at a Hacker conference between 2016-2019

Interview #4: nonprofit technologist, digital security trainer, conducted at a Hacker conference between 2016-2019

Interview #5: digital security trainer, NGO founder, conducted at a Hacker conference between 2016-2019

Interview #6: digital security trainer, Lawyer, LGBTQIA+ activist, conducted at a Digital Rights Conference between 2016-2019

Interview #7: user experience specialist, nonprofit technologist, conducted at a Digital Rights Conference between 2016-2019

Interview #8: digital security trainer, facilitator, nonprofit technologist, conducted at a Digital Rights Conference between 2016-2019

Interview #9: digital security trainer, facilitator, conducted at a Digital Rights Conference between 2016-2019

Interview #10: digital security trainer, feminist & women's rights activist, conducted at a Digital Rights Conference between 2016-2019

Interview #11: digital security trainer, conducted at a Digital Rights Conference between 2016-2019

Interview #12: digital security specialist, nonprofit technologist, conducted at a Digital Rights Conference between 2016-2019

Interview #13: digital security trainer, feminist activist, conducted at a Digital Rights Conference between 2016-2019

Interview #14: nonprofit technologist, digital security trainer, conducted at a Digital Rights Conference between 2016-2019

Interview #15: lawyer, digital security specialist, conducted at a Digital Rights Conference between 2016-2019

Interview #16: computer science professor, conducted at a FLOSS project meeting between 2016-2019

Interview #17: labor activist, digital security trainer, conducted at a grassroots technology festival between 2016-2019

Interview #18: nonprofit technologist, open source investigator, conducted at a grassroots technology festival between 2016-2019

Interview #19: computer science professor, conducted at a Hacker Camp between 2016-2019

Interview #20: Governmental cybersecurity specialist, conducted at a Hacker Camp between 2016-2019

Interview #21: commercial cybersecurity specialist, conducted at a Hacker Camp between 2016-2019

Interview #22: two tech activists & security researchers, conducted at a Hacker Camp between 2016-2019

Interview #23: commercial telecommunications worker, conducted at a Hacker Camp between 2016-2019

Interview #24: nonprofit technologist, conducted at a Hacker Camp between 2016-2019

Interview #25: computer science professor, conducted at a Hacker Camp between 2016-2019

Interview #26: FLOSS volunteer, conducted at a Hacker Camp between 2016-2019

Interview #27: FLOSS ‘user’ conducted at a Hacker Camp between 2016-2019

Interview #28: governmental Cybersecurity specialist, conducted at a Hacker Camp between 2016-2019

Interview #29: governmental Cybersecurity specialist, conducted at a Hacker Camp between 2016-2019

Interview #30: nonprofit technologist, security researcher, conducted at a Hacker Camp between 2016-2019

Interview #31: journalist, digital security practitioner, conducted at a digital security training between 2016-2019

Interview #32: journalist, digital security practitioner, conducted at a digital security training between 2016-2019

Interview #33: two environmental rights NGO workers, conducted at a digital security training between 2016-2019

Interview #34: human rights defender, conducted at a digital security training between 2016-2019

Interview #35: human rights defender and NGO founder, conducted VOIP between 2016-2019

Interview #36: feminist and women's rights activist and psychosocial security trainer, conducted at a Digital Rights Conference between 2016-2019

Interview #37: human rights defender, journalist, and digital security trainer, conducted at a Digital Rights Conference between 2016-2019

Interview #38: feminist and women's rights activist and digital security trainer, conducted at a Digital Rights Conference between 2016-2019

Interview #39: feminist and women's rights activist and digital security specialist, conducted at a Digital Rights Conference between 2016-2019

Interview #40: feminist grassroots technologist, conducted at a Digital Rights Conference between 2016-2019

Interview #41: lawyer and digital security trainer, conducted VOIP between 2016-2019

Interview #42: nonprofit digital security specialist and NGO founder, conducted at a Digital Rights Conference between 2016-2019

Interview #43: nonprofit digital security specialist and NGO founder, conducted at a Digital Rights Conference between 2016-2019

Interview #44: abolitionist community organiser, conducted at a Digital Rights Conference between 2016-2019

Interview #45: NGO founder, conducted VOIP between 2016-2019

Interview #46: nonprofit technologist and FLOSS volunteer, conducted at a FLOSS meeting between 2016-2019

Interview #47: two nonprofit technologists, conducted at a hacker space between 2016-2019

2. Interview Questions

Example interview questionnaire with digital security trainer

1. What inspired you to start working on digital security?
2. Which projects do you work on/organisations do you work with?
3. What drew you to work on these specifically?
4. What do you think are the most important security problems at the moment?
5. Which technological/security/privacy risks and threats concern you most as a trainer/security specialist?
6. What is your audience / target group? What kind of people do come to your trainings?
7. What is the format of the intervention?
8. What ideas do you try to get across?
9. What kinds of concerns do the people have who participate in your trainings?
10. What kind of feedback do you get on your training?
11. As far as you know, do people change their practices following the training?
12. How do you determine which security problems to focus on for the people you work with
13. Do you follow a formalised process?
14. Do you try to assess risk?
15. If so, do you try to measure or calculate security risks and threats?

16. What tools do you teach or not teach? Why? (going into specifics of each tools)
17. What are benefits of this tool? What are the challenges of its use?
18. Why/do you promote this tool with the communities you work with?
19. How do or can trainers contribute to the usability of tools?
20. What are the challenges of adopting these practices, for the people who come?
21. What moments or challenges have required you to rethink how you teach security practices
22. How should challenging security practices best be integrated into everyday life?
23. How do you translate technical concepts, problems and solutions, between more and less technology-focused people?
24. Do you use these tools in your own practices?
25. What moments or challenges have required you to rethink your practices?
26. What does a long term view look like for the communities you work with?
27. What do you think will need to be prioritized in coming years?

Example interview questionnaire with technologist developing Free/Libre Open Source security software

1. What inspired you to start working on security?
2. Which projects do you work on? What drew you to work on these specifically?
3. What do you think are the most important security problems at the moment?
4. What do you think are the most persistent problems relating to security and security software design?
5. What risks and threats do you worry about most as a security professional?

6. How do you determine security requirements/priorities for the tools you develop?
7. Is there a formalised process?
8. Do you try to measure or calculate security risks and threats?
9. Do you use specific forms of security analysis like threat modelling in your tool development?
10. What concepts and principles are central to the tool/platform/projects you contribute to?
11. How have the security priorities for the tools you work on evolved over their development?
12. What does a long term view look like for the projects you work on?
13. What issues do you think will be need to be prioritized in coming years?
14. How do you see your work in elation to the commercial security industry?
15. Are there pans for any of these projects to get turned into products?
16. What are the challenges of working on FLOSS projects in particular?
17. Who do you develop your tools for?
18. Are tool usability issues a part of your concern as a developer?
19. Do you talk to users of the software about their experiences?
20. Do you use these tools in your own digital practices?
21. What moments or challenges have required you to rethink your own digital practices?

3. Research Participant Information Sheet

DATACTIVE is an interdisciplinary research collective based at the University of Amsterdam. We investigate grassroots engagement with massive data collection. Our research is funded by the European Research Council.

What is DATACTIVE about?
We investigate grassroots engagement with massive data collection. With the progressive datafication of many aspects of human life, people become increasingly aware of the critical role of information in modern societies. This awareness nurtures new socio-technical practices rooted in data and technology, for which we use the notion of 'data activism'. By increasingly involving ordinary users, data activism signals a change in perspective and attitude towards datafication and massive data collection emerging within the civil society realm.

How do we work?
We experiment with engaged research, an approach to research that, without departing from systematic, evidence-based, social science research, aims to make a difference for groups and individuals beyond the academic community. This approach emerges from our individual engagement over the years with a variety of social movements and non-governmental organizations across the world. It affects, for example, the questions we ask and the ways we engage with groups and individuals. We explicitly privilege a grassroots perspective, and our research often takes sides. It is activism by other means.

We take the ethics of research very seriously

- we remove identifying details that might contribute to the vulnerability of persons and projects
- we provide full anonymity to interviewees on an individual level*
- we store and share all data that we collect with strong encryption
- we share and discuss research outputs with interviewees before they are published
- we strive to write and publish our research in an accessible way

- we design our protocols in consultation with our Ethics Board

Would you like to contribute?

Our methods mirror these commitments. When engaging in an interview with us

- you can use a pseudonym
- you can ask your own questions to us
- you are free not to answer questions you are not comfortable with
- your data will not be shared with third parties
- you will receive information about how you data will be used in the research
- Our research depends on your participation, and we look forward to exchanging ideas with you.

* unless otherwise requested by the interviewee

4. Coding scheme with main themes & sub-themes

Anticipatory logics & orientations	anticipation preemption prediction prevention resilience awareness & vigilance proactivity
threats	Targeted surveillance attacks by state-sponsored actors Gendered online/offline violence & harassment Disinformation & defamation attacks against civil

	society groups Distributed denial of service attacks Internet of things data exploitation Malware attacks targeting civil society organizations garden-variety malware concerns physical surveillance biometric surveillance: facial recognition corporate data exploitation i.e. Facebook policies discrimination by automated systems predictive/preemptive policing preemptive office raids
Resistant Practices, tactics & strategies	threat modelling risk assessment developing new security standards developing threat taxonomies & ontologies engaging in threat intelligence sharing running help desks for rapid response to digital threats trainings + awareness raising interventions feminist pedagogies around technology: new lexicons, ontologies compartmentalization strategies for computing systems & activists user-centred control of IoT networked devices obfuscation techniques for data & facial recognition tech structured security protocols for NGOs threat information sharing platform development automated, data-driven security prediction suing the police as part of abolitionist strategizing
Threat response orientations	resignation refusal

(affective, epistemological, socio-material & value-driven)	appropriation re-configuration prefiguration feminist data & security epistemologies (embodiment, de-militarization) civil society digital security tropes state-centric cybersecurity tropes (cyberspace & warfare discourse; norms, standards development) commercial cybersecurity tropes (automation, centralization, assetisation)
Scale/scope of work of collaborations, projects, organizations	local national regional transnational trans-local trans-regional
Relations between groups, projects, infrastructures	Contestation Collaboration/coordination
Civil Society self-definitions	Field of work digital security training digital rights advocacy privacy activism human rights defense Internet freedom circumvention technology development technical service provision intermediary/support work social justice

	social movements anticorruption land rights women’s rights LGBTQIA+ rights gender equality environmental rights antiracism anti-descrimination labor union organizing anti-carceral tech abolitionist community organizing FLOSS software development journalism Organization institutionalization nonprofit organization for-profit consultancy grassroots collective tech project/software project state cybersecurity incident response organization Individual identification FLOSS technology developer security educator security expert security specialist technological service provider hacker community organizer human rights defender digital rights defender land rights defender environmental rights defender

	women's rights defender feminist/gender equality defender LGBTQIA+ rights defender anti-corruption activist journalist
Civil society field priorities	funding (sustainability, social dynamics) professionalization (development of expertise & structured protocols) efficiency of threat response (rapid response, infrastructure maintenance diversity of experts, grantees, representatives (racial, socio-economic, geographic, gender) racism & anti-racism as strategies/ issues endemic to civil society work adapting to shifting digital & surveillance-related threats engaging with persistent problems amidst a quickly shifting attention economy epistemic justice between rich NGOs in US and Europe vs organizations in the majority world mainstreaming of feminist epistemologies
Tensions & Controversies in civil society	emphasis on self defense vs. an emphasis on policy advocacy politics of data vs tool-driven fixes tactics vs. strategies global, transnational vs. local, trans-local qualitative vs. quantitative approaches to managing risk centralized vs. decentralized security infrastructures totalist vs contingent + contextualized understandings of surveillance human rights vs. social justice framing for advocacy reform vs. abolition oriented strategies of resistance

	belonging to civil society vs belonging to 'movements' or 'communities' privacy: individual versus collective security: digital security vs cybersecurity safety: community versus top down focusing on fixing persistent day-today problems vs raising awareness of speculative, emerging concerns

References

Abrahamsen R and Williams M (2011) Security Privatization and Global Security Assemblages. *The Brown Journal of World Affairs,* 18(1): 171-180.

Acquisti A (2010) From the Economics to the Behavioral Economics of Privacy: A Note. In: Kumar A., Zhang D (eds) Ethics and Policy of Biometrics. ICEB 2010. *Lecture Notes in Computer Science.* 6005. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-12595-9_4

Acquisti A and Grossklags J (2007) What can behavioral economics teach us about privacy. In: De Capitani di Vimercati S, Gritzalis S, Lambrinoudakis C, et al. (eds) *Digital Privacy: Theory, Technologies and Practices.* Auerbach Publications, pp. 363–377.

Adams A and Sasse MA (1999) Users are not the enemy: Why users compromise computer security mechanisms and how to take remedial measures. *Communications of the ACM*, 42(12): 40–46, December 1999.

Adams V, Murphy M and Clarke AE (2009) Anticipation: Technoscience, life, affect, temporality. *Subjectivity* 28: 246–265.

Ahmed N and Aoun S (2018) Please Don't Include Us Thank You. In: *Theorizing the Web*, New York, 27 April 2018.

Alvial-Palavicino C (2015) The future as practice. A framework to understand anticipation in science and technology. *Tecnoscienza* 6(2): 135–172.

Amnesty International (2017) Human Rights Defenders Under Threat – a shrinking space for civil society. Report, Amnesty International Ltd London. Available at: https://www.amnesty.nl/content/uploads/2017/05/HRD-briefing-26-April-2017-FINAL.pdf?x18276 (accessed March 5 2021).

Amoore L (2013) *The Politics of Possibility: Risk and Security beyond Probability.* Durham, NC: Duke University Press.

Amoore L (2020) *Cloud Ethics*. Durham, NC: Duke University Press.

Amoore L and de Goede M (2008) *Risk and the war on terror*. London: Routledge.

Amoore L and Langley P (2004) *Ambiguities of Global Civil Society.* Review of International Studies, 30(1): 89-110.

Amsler S and Facer K (2017) Contesting anticipatory regimes in education: Exploring alternative educational orientations to the future. *Futures.* https://doi.org/ 10.1016/j.futures.2017.01.001

Anderson B (2007) Hope for nanotechnology: Anticipatory knowledge and the governance of affect. *Area* 39(2): 156–165.

Anderson B (2010) Preemption, precaution, preparedness: Anticipatory action and future geographies. *Progress in Human Geography* 34(6): 777–798.

Anderson B and Adey P (2011) Anticipating emergencies: Technologies of preparedness and the matter of security. *Security Dialogue* 43(2): 99-117.

Andrejevic M (2005) The Work of Watching One Another: Lateral Surveillance, Risk, and Governance. *Surveillance & Society* 2(4): 479–97

Andrejevic M (2017) To pre-empt a thief. I*nternational Journal of Communication* (11): 879–896.

Andrejevic M, Dencik L and Trere, E (2019) From preemption to slowness: assessing the contrasting temporalities of data-driven predictive policing. *New Media and Society* 22(9): 1528-1544.

Andrejevic M (2019). *Automated media*. London & New York: Routledge.

Annany M and Finn M (2020) Anticipatory news infrastructures: Seeing journalism's expectations of future publics in its sociotechnical systems. *New media & society* 22(9) 1600–1618

Aouragh M, Gürses S, Rocha J, et al. (2015) Let's first get things done! On division of labour and techno-political practices of delegation in times of crisis. *Fibreculture Journal* (26): 208–235. DOI: 10.15307/fcj.26.196.2015

Aradau C (2018) Governing others: Anomaly and the algorithmic subject of security. *European Journal of International Security* 3(1): 1-21.DOI:10.1017/eis.2017.14

Aradau C and Blanke T (2017) Politics of prediction: Security and the time/space of governmentality in the age of big data. *European Journal of Social Theory* 20(3): 373–391.

Aradau C and van Munster R (2008) Taming the Future: The Dispositif of Risk in the War on Terror. In: Amoore L and de Goede M (eds). *Risk and the War on Terror*. London, UK: Routledge.

Aradau C and van Munster R (2012) The Time/Space of Preparedness: Anticipating the "Next Terrorist Attack". *Space and Culture* 15(2): 98–109. DOI: 10.1177/1206331211430015.

APC Women's Rights Programme Feminist Tech eXchange (2019). Available at: https://www.apc.org/en/project/feminist-tech-exchange (accessed 5 August 2020).

Asgharpour F, Liu D and Camp LJ (2007) Mental models of computer security risks. In Proceedings of the 6th annual workshop on the economic of information security (WEIS 2007).

Baek G and Mooney T (2020) LAPD not giving up on data-driven policing, even after scrapping controversial program. *CBS news,* 23 February, 2020.

Ballestero A (2015) The ethics of a formula: calculating a financial-humanitarian price for water American. Ethnologist 42 (2): 262-278

Ball K and Snider L (eds) (2013) *The Surveillance-Industrial Complex: A Political Economy of Surveillance*. London: Routledge.

Baker K (2021) What is Cyber Threat intelligence? Available at: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/ (accessed 1 August 2021).

Barnard-Wills D (2012) E-safety education: Young people, surveillance and responsibility. *Criminology & Criminal Justice* 12(3):239-255. DOI:10.1177/1748895811432957

Bauman Z, Bigo D, Esteves P, et al. (2014) After Snowden: Rethinking the impact of surveillance. *International Political Sociology* 8(2): 121-144.

Baumer EPS, Ames, MG, Burrell J, et al. (2015) Why study technology non-use? *First Monday* 20 (11 – 2). http://dx.doi.org/10.5210/fm.v20i11.6310

Beck U (1992) *Risk Society: Toward a New Modernity.* New York: Sage.

Bellanova R and de Goede M (2020) The Algorithmic Regulation of Security: An Infrastructural Perspective. *Regulation & Governance.* https://doi.org/10.1111/rego.12338

Benjamin R (2016) Informed Refusal: Toward a Justice-Based Bioethics. *Science, Technology, & Human Values* 41(6): 967–90. https://doi.org/10.1177/0162243916656059

Benjamin R (2019) *Race after Technology: Abolitionist Tools for the New Jim Code*. Cambridge, MA: Polity.

Beraldo D and Milan S (2019) From data politics to the contentious politics of data. *Big Data & Society*. https://doi.org/10.1177/2053951719885967

Bigo D (2006) Globalized in-security: The field of the professionals of unease management and the Ban- opticon. In: Solomon J and Sakai N (eds) *Traces: A Multilingual Series of Cultural Theory* 4 (Translation, Philosophy and Colonial Difference). Hong Kong: University of Hong Kong Press, pp. 109–157.

Boggs C (1977) Marxism, prefigurative communism and the problem of workers' control. Radical America, 6(Winter): 99– 122.

Blythe J and Camp LJ (2012) Implementing mental models. In: IEEE Symposium on Security and Privacy Workshops, pp. 86–90. IEEE Computer Society.

Body & Data (year unknown). Available at: https://bodyanddata.org/ (accessed 18 January 2021).

boyd d (2008) *Taken out of context: American teen sociality in networked publics*. PhD Dissertation, University of California Berkeley.

Bouk D (2015) *How Our Days Became Numbered: Risk and the Rise of the Statistical Individual*. Chicago: University of Chicago Press.

Bourbeau B (2018) A Genealogy of Resilience. I*nternational Political Sociology.* 12(1): 19–35. https://doi.org/10.1093/ips/olx026

Bowker G and Star SL (1999) *Sorting Things Out: Classification and Its Consequences*. Cambridge, MA: The MIT Press.

Brand S and Sander I (2020) *Critical data literacy tools for advancing data justice: A guidebook.* Data Justice Lab, Cardiff, Wales, UK. Available at: https://datajustice.files.wordpress.com/2020/06/djl-data-literacy-guidebook.pdf (accessed 4 December 2020).

Braun V and Clarke V (2019) Reflecting on reflexive thematic analysis. *Qualitative Research in Sport, Exercise and Health* 11(4): 589-597. DOI:10.1080/2159676X.2019.1628806

Braun V and Clarke V (n.d.) Thematic analysis | a reflexive approach. Available at: https://www.psych.auckland.ac.nz/en/about/thematic-analysis.html

Brayne S (2017) Big data surveillance: the case of policing. *American Sociological Review* 82: 977–1008.

Brayne S (2020) *Predict and Surveil. Data, Discretion, and the Future of Policing.* Oxford University Press.

Brown D and Pytlak A (2020) Why Gender Matters in International Cyber Security. Report, Association for Progressive Communications, April. Available at: https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security (accessed 3 July 2020).

Browne S (2015) *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Brooks S (2019) Defending Politically Vulnerable Organizations Online. Report, Center for Long-term Cybersecurity. Available at: https://cltc.berkeley.edu/2018/07/24/defending-politically-vulnerable-organizations-online/ (accessed 8 March 2019).

Brunton F and Nissenbaum H (2015) *Obfuscation: A User's Guide for Privacy and Protest.* Cambridge, MA: MIT Press.

Bucher T (2017) The algorithmic imaginary: exploring the ordinary affects of Facebook algorithms. *Information, Communication & Society* 20(1): 30–44.

Buolamwini J and Gebru T (2018) Gender shades: Intersectional accuracy disparities in commercial gender classification. Conference on fairness, accountability and transparency (2018), pp. 77-91 (January).

Burrell J (2009) The Field Site as a Network: A Strategy for Locating Ethnographic Research. *Field Methods* 21(2): 181–99.

Callon M and Law J (2005) On Qualculation, Agency, and Otherness. *Environment and Planning D: Society and Space* 23(5):717-733. DOI:10.1068/d343t

Carmi E, Yates S and Pawluczuk A et al. (2020) Data citizenship: rethinking data literacy in the age of disinformation, misinformation, and malinformation. *Internet Policy Review* [online] 9(2). Available at: https://policyreview.info/articles/analysis/data-citizenship-rethinking-data-literacy-age-disinformation-misinformation-and

Castoriadis C (2005) *The Imaginary Institution of Society*. Cambridge: Polity Press.

Chan SA (2013) *Networking Peripheries. Technological Futures and the Myth of Digital Universalism*. Cambridge: MIT Press.

Citizen Lab (2014) Extended analysis: Civil society perspectives and responses. Communities @ Risk: Targeted Digital Threats Against Civil Society. Report, Citizen Lab, University of Toronto. Available at: https://targetedthreats.net/media/2.3%20Extended%20Analysis-CivilSociety.pdf (accessed 23 December 2020).

Clarke AE (2015) Anticipation work: Abduction, simplification, hope. In: Bowker, GC, Timmermans, S, Clarke, AE, et al. (eds) *Boundary Objects* *and Beyond: Working With Leigh Star* (pp. 85–120). Cambridge: MIT Press.

Clark-Ginsberg B and Slayton R (2017) A Innovation or Maintenance? The Creation and Evolution of Critical Infrastructure Cybersecurity Standards.

Coaffee J (2013) Rescaling and Responsibilising the Politics of Urban Resilience: From National Security to Local Place-Making. *Politics* 33(4): 240–252.

Cochoy F (2008) Calculation, qualculation, calqulation: shopping cart arithmetic, equipped cognition and the clustered consumer. *Marketing Theory*. 8(1):15-44. DOI:10.1177/1470593107086483

Coding Rights (year unknown) Safer Nudes. Available at: https://www.codingrights.org/safernudes/ (accessed June 20, 2019).

Coleman G (2013) *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton, NJ: Princeton University Press.

Costanza-Chock, S, Wagoner, M, Taye, B, et al. (2018) #MoreThanCode: Practitioners Reimagine the Landscape of Technology for Justice and Equity. Report, Research Action Design & Open Technology Institute, Washington, DC, USA.

Cox J (2014) The rise of the anti-facial recognition movement. In: *The Kernel*. Available at: https://kernelmag.dailydot.com/issue-sections/features-issue-sections/10247/ anti-facial-recognition-movement

Couldry N and Powell A (2014) Big data from the bottom up. *Big Data & Society* 1(2): 1–5. https:// doi.org/10.1177/2053951714539277.

Couture S and Toupin S (2019) What does the notion of “sovereignty” mean when referring to the digital? *New Media & Society*. 21(10): 2305-2322. DOI: 10.1177/1461444819865984

Crawford K (2019) Halt the use of facial-recognition technology until it is regulated. *Nature* 572(7771): 565. Available at: https://www.nature.com/articles/d41586-019-02514-7 (accessed 21 January 2020).

Critical Arts Ensemble (2001) *Digital Resistance. Explorations in Tactical Media*. New York: Autonomedia.

Critical resistance (2021) History. Available at: http://criticalresistance.org/about/history/ (accessed 3 May 2019).

Daskal E (2018) Let’s be careful out there...: how digital rights advocates educate citi- zens in the digital age. *Information, Communication & Society* 21(2): 241–256.

Datafication and Community Activism Workshop (2019) What we mean when we say #AbolishBigData2019. Medium. Mar. 22. Available at: https://medium.com/@rncrooks/what-we-mean-when-we-say-abolishbigdata2019-d030799ab22e

Davis A and Mendieta E (2005) *Abolition Democracy: Beyond Empire, Prisons, and Torture*. New York: Seven Stories.

de Goede M (2004) Repoliticising financial risk. *Economy and Society* 33(2): 197-217.

de Goede M (2008) The politics of preemption and the War on Terror in Europe. *European Journal of International Relations* 14(1): 161-185.

de Goede M (2012) *Speculative Security: The Politics of Pursuing Terrorist Monies.* Minneapolis: University of Minnesota Press.

de Goede M (2014) Preemption Contested: Suspect Spaces and Preventability in the July 7 Inquest. *Political Geography* 39: 48-57.

de Goede M (2014) The politics of privacy in the age of preemptive security. *International Political Sociology* 8(1): 100-104.

de Goede M, Simon S and Hoijtink M (2014). Performing preemption. Security Dialogue, 45(5): 411-422. https://doi.org/10.1177/0967010614543585

de Goede M and Randalls S (2009) Preemption, Precaution: Arts and Technologies of the Governable Future. *Environment and Planning D: Society and Space* 27(5): 859-878.

De Filippi P and Treguer F (2014) Expanding the Internet commons: The subversive po- tential of wireless community networks. *Journal of Peer Production* 6. Available at: http://peerproduction.net/wp-content/uploads/2015/01/De-Filippi-Tréguer-Ex- panding-the-Internet-Commons-with-Community-Networks.pdf

De Hert P and Vis T (2005) Intelligence led policing ontleed. *Tijdschrift voor Criminologie* 47(4): 365 – 376.

Deleuze G (1992) Postscript on the societies of control. *October* 59(1): 3–7.

Della Porta D, Peterson A and Reiter, H (2006) (eds) *The Policing of Transnational Protest.* Farnham: Ashgate.

Della Porta D and Reiter H (1998) *Policing protest: The control of mass demonstrations in Western democracies*. Minneapolis: University of Minneapolis Press.

Dencik L, Hintz A and Cable J (2016) Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society* 3(2): 1–12. DOI: 10.1177/2053951716679678.

Dencik L and Cable J (2017) The Advent of Surveillance Realism: Public Opinion and Activist Responses to the Snowden Leaks. *International Journal of Communica tion* 11: 763–781.

Dencik L, Hintz A, Carey Z et al. (2015) Managing 'threats': uses of social media for policing domestic extremism and disorder in the UK. Report, Cardiff University, Wales.

Dencik, L, Hintz, A, Carey, Z (2017) Prediction, preemption and limits to dissent: Social media and big data uses for policing protests in the United Kingdom. New Media & Society 20(4): 1433–1450.

Decnik L, Hintz A, Redden J et al. (2019). Data Scores as Governance: Investigating uses of citizen scoring in public services. Report, Data Justice Lab, Cardiff University, Wales, December.

De Vries P and Schinkel W (2019) Algorithmic anxiety: Masks and camouflage in artistic imaginaries of facial recognition algorithms. *Big Data and Society*. https:// doi.org/10.1177/2053951719851532.

Didier E (2018) Globalization of Quantitative Policing: Between Management and Statactivism. *Annual Review of Sociology* 44(1): 515-534.

D'Ignazio C (2017) Creative Data Literacy. *Information Design Journal* 23(1): 6-18.

D'Ignazio C and Klein L (2020) *Data Feminism.* Cambridge, MA: MIT Press.

Doringer B and Felderer B (eds) (2018) *Faceless. Re-Inventing Privacy Through Subversive Media Strategies*. Berlin: De Gruyter.

Douglas M (1992) *Risk and Blame: Essays in Cultural Theory*. London, UK: Routledge.

Dourish P, Grinter R, de la Flor D, et al. (2004). Security in the wild: User strategies for managing security as an everyday, practical problem. *Personal and Ubiquitous Computing* 8(6): 19-30.

Dowse (n.d.) What is Dowse? Available at: http://www.dowse.eu/faq/.

Draper NA and Turow J (2019) The corporate cultivation of digital resignation. *New Media & Society* 21(8): 1824–1839.

Dyne.org Foundation (2017) Dowse Whitepaper (v 1.2). Available at: https://files.dyne.org/dowse/dowse_whitepaper.pdf (accessed 3 March 2018).

Duffield M (2010) Risk-management and the fortified aid compound: Everyday life in post-interventionary society. *Journal of Intervention and Statebuilding* 4(4): 453–474.

Duffy BE and Chan, NK (2018) "You never really know who's looking": Imagined surveillance across social media platforms. *New Media & Society* 21(1): 119–138.

Dunbar-Hester C (2014) *Low Power to the People.* Cambridge, MA: MIT Press.

Dunbar-Hester C (2019) *Hacking Diversity: The Politics of Inclusion in Open Technology Cultures.* Princeton, NJ: Princeton University Press.

Dunn Cavelty M (2013) From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review* 15(1): 105–122. DOI:10.1111/misr.12023

Dwyer AC (2019) *Malware ecologies: a politics of cybersecurity* [PhD thesis]. Oxford, UK: University of Oxford.

Dyer-Witheford N and Matviyenko S (2019) *Cyberwar and Revolution: Digital Subterfuge in Global Capitalism*. Minneapolis, Minnesota: University of Minnesota Press.

Enslev L, Mirsal L and Winthereik BR (2018) Anticipatory infrastructural practices: The coming of electricity in rural Kenya. *Energy Research & Social Science*(44): 130-137.

Elder M (2013) Russia raids human rights groups in crackdown on 'foreign agents.'*The Guardian*. 27 March. Available at: https://www.theguardian.com/world/2013/mar/27/russia-raids-human-rights-crackdown (accessed 1 March 2021).

Emmer P, Rivas, C, Neves, BS; Schweidler, C (2020) Technologies for Liberation: Toward Abolitionist Futures. Report, Astraea Lesbian Foundation for Justice and Research Action Design, December. Available at: astraeafoundation.org/FundAbolitionTech

Epstein B (1991) *Political protest and cultural revolution.* Berkeley: University of California Press.

Enslev L, Mirsal L and Winthereik BR (2018) Anticipatory infrastructural practices: The coming of electricity in rural Kenya. *Energy Research & Social Science* (44): 130-137.

Enterprise Risk Management Initaitive (2008) Eight Principles of Risk Convergence and Implications for GRC Technology Solutions. Available at: https://erm.ncsu.edu/library/article/GRC-technology-solutions (accessed 3 April 2021).

Earl S, Carden F, Smutylo T (2001) *Outcome Mapping.* Ottawa: International Development Research Centre.

Electronic Frontier Foundation (year unknown). Surveillance Self Defense. Available at: https://ssd.eff.org (accessed 29 June 2017).

Ermoshina K and Musiani F (2018) Hiding from whom? Threat models and in-the-Making encryption technologies. I*ntermédialités.* DOI: 10.7202/1058473ar.

Ettlinger N (2018) Algorithmic affordances for productive resistance. *Big Data & Society*. https://doi.org/10.1177/2053951718771399

Eubanks V (2011) Popular Technology. In Digital Dead End: Fighting for Social Justice in the Information Age (pp. 99-128). Cambridge, Massachusetts; London, England: The MIT Press.

Eubanks V (2018) Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York, NY: St. Martin's Press.

Face Dazzler (n.d.) Counter Facial Recognition. Available at: http://facedazzler.zweis- tein.cz (accessed 5 March 2018).

Faulkner SL and Trotter SP (2017) Data Saturation. In The International Encyclopedia of Communication Research Methods (eds Matthes J, Davis CS and Potter, RF). https://doi.org/10.1002/9781118901731.iecrm0060

Fichtner L (2018) What kind of cyber security? Theorising cyber security and mapping approaches. I*nternet Policy Review* 7(2). https://doi.org/10.14763/2018.2.788

FIRST (2016) FIRST announces Traffic Light Protocol (TLP) version 1.0. Available at: https://www.first.org/newsroom/releases/20160831 (accessed 23 September 2019).

Fernandez, E, Caraj, M (2009) The New Protection Manual for Human Rights Defenders. Report, Protection International, Brussels.

Fernandez LA and Huey L (2009) Is Resistance Futile? Some Thoughts on Resisting Surveillance. *Surveillance & Society* 6(3): 198-202.

Ferreira A, Huynen JL, Koenig V, et al. (2014) A conceptual framework to study socio-technical security. In: Human Aspects of information security, Privacy, and Trust. Los Angeles, HAS: International Conference on Human Aspects of Information Security, Privacy, and Trust, pp 318–329. doi:10.1007/978-3-319-07620-1_28

Flichy P (2007) *The Internet Imaginaire*. Cambridge, MA: MIT Press.

Fotopoulou A (2014) Digital and networked by default? Women's organisations and the social imaginary of networked feminism. *New Media & Society* 18(6): 989–1005.

Front Line Defenders (2011) *Workbook on Security: Practical Steps for Human Rights Defenders at Risk.* Dublin Ireland: Front Line.

Funnell, A (2015) Predictive Policing: Putting Data on the Beat. Future Tense [Radio show]. Aired on August 23, 2015 on ABC Radio National, Australia. Available at: http://www.abc.net.au/radionational/programs/futuretense/predictive-policing3a-putting-data-on-the-beat/6702640#transcript (accessed 13 May, 2019).

Gabrys J (2017) Citizen sensing, air pollution and fracking: From 'caring about your air' to speculative practices of evidencing harm. *The Sociological Review Mono- graphs* 65(2):172–192.

Galvez R and Gürses S (2018) The Odyssey: Modelling privacy threats in a brave new world. In: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, 2018, pp. 87–94. DOI: 10.1109/EuroSPW.2018.00018.

Gandy OH (1993) *The Panoptic Sort: A Political Economy of Personal Information.* Boulder, Colorado: Westview.

Gandy OH (2009) *Coming to Terms with Chance: Engaging Rational Discrimination and Cumulative Disadvantage.* Routledge.

Gangadharan SP, Niklas J (2018) Between Antidiscrimination and Data: Understanding Human Rights Discourse on Automated Discrimination in Europe. Report, London School of Economics, London, UK, May.

Gangadharan SP (2020) Digital exclusion: a politics of refusal. In: Landemore H, Reich R, and Bernholz, L (eds.) Digital Technology and Democratic Theory. Chicago: University of Chicago Press, preprint.

Gaw S and Felten EW (2006) Password Management Strategies for Online Accounts. In: Proceedings of the 2nd Symposium on Usable Privacy andSecurity, ser. SOUPS '06, pp. 44–55.

Gillham PF (2011) Securitizing America: Strategic incapacitation and the policing of protest since the 11 September 2001 terrorist attacks. *Sociology Compass* 5(7): 636–652.

Gilmore RW (2007) *Golden Gulag: Surplus, Crisis, and Opposition in Globalizing*. Berkeley and Los Angeles, CA: University of California Press.

Gürses S (2014) Attitudes Towards "Spiny CACTOS. Available at: http://vous-etes-ici.net/?p=80. (Accessed: 9 March 2015).

Gürses S, Kundnani A, van Hoboken J (2016) Crypto and empire: The contradictions of counter-surveillance advocacy. *Media, Culture and Society* 38(4): 576–590.

Gürses S, Overdorf R and Balsa E (2018) POTs: The revolution will not be optimized? In: *Proceedings on Privacy Enhancing Technologies Symposium*, 2018. Available at: https://www.petsymposium.org/2018/files/hotpets/3-gurses.pdf.

Gutiérrez M and Milan S (2019) Playing with data and its consequences. *First Monday* 24(1). https://doi.org/10.5210/fm.v24i1.9554 [details]

Haché A 2014) La Souveraineté technologique (Vol. 1). Dossier ritimo. Available at: .

Haché A (2018) La Souveraineté technologique—Volume 2. Dossier ritimo. Available at: .

Hackblossom.org (n.d.) A DIY Guide to Feminist Cybersecurity. Available at: https://hackblossom.org/cybersecurity/

Hacking I (1975) *The Emergence of Probability.* Cambridge: Cambridge University Press.

Hamid ST (2020 Community defense: Sarah T. Hamid on abolishing carceral technologies. *Logic Magazine,* 31 August. Available at: https://logicmag.io/care/community-defense-sarah-t-hamid-on-abolishingcarceral-technologies/

Hankey S and Ó'Clunaigh D (2013) Rethinking risks and security of human rights defenders in the digital age. *Journal of Human Rights Practice* 5(3): 535–547.

Hansen L and Nissenbaum H (2009) Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly* 53(4): 1155–1175. DOI:10.1111/j.1468-2478.2009.00572.x

Haraway D (1988) Situated knowledges: The science question in feminism and the privilege of partial perspective. *Feminist Studies* 14(3): 575-599.

Haraway D (2016) Staying with the trouble. In: J.W. Moore, (ed) *Anthropocene or capitalocene?* Oakland: PM Press, pp. 34–76.

Hardt M and Negri M (2004) *Multitude: War and democracy in the age of empire.* New York, The Penguin Press. Koskela, Hille. 2004. Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism. Surveillance & Society 2(2/3): 199- 215.

Harvey P, Reeves M and Ruppert E (2012) Anticipating Failure: Transparency Devices and their Effects. *Journal of Cultural Economy* 6(4): 1–19.

Hellegren ZI (2017) A history of crypto-discourse: encryption as a site of struggles to de-fine internet Internet freedom. *Internet Histories* 1(4): 285–311. DOI: 10.1080/24701475.2017.1387466. c

Hintz A and Brown I (2017) Enabling Digital Citizenship? The Reshaping of Surveillance Policy After Snowden. *International Journal of Communication* 11: 782–801.

Hintz A and Milan S (2010) Social science is police science: researching grass-roots activism. *International Journal of Communication* 4: 837–844.

Hintz A and Milan S (2013) Networked collective action and the institutionalised policy debate: Bringing cyberactivism to the policy arena? *Policy & Internet* 5(1): 7–26.

Hintz A and Milan S (2018) Through a glass, darkly: Everyday acts of authoritarianism in the liberal West. *International Journal of Communication* 12: 3939–3959.

Hoffmann AL (2019) Where fairness fails: data, algorithms, and the limits of antidiscrim- ination discourse. *Information, Communication & Society* 22(7): 900–915.

Hoffman A (2020). Terms of Inclusion: Data, Discourse, Violence. *New Media & Society.* DOI: 10.1177/1461444820958725.

Hong S (2015) Subjunctive and interpassive knowing in the surveillance society. *Media and Communication* 3(2): 63–76.

Horgan, L and Dourish, P (2018). Ambiguity, Ambivalence, and Activism: Data Organizing Inside the Institution. *Krisis: Journal for Contemporary Philosophy,* Data Activism, no. 1.

Human Rights Watch (2020) India: Counterterrorism Raids Targeting Peaceful Critics, 30 October. Available at: https://www.hrw.org/news/2020/10/30/india-counterterrorism-raids-targeting-peaceful-critics,(accessed 2 March 2021).

Ioannis A, Nurse, JRC, Goldsmith M, Creese S, Upton, D (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity* 4(1). https://doi.org/10.1093/cybsec/tyy006

Jasanoff S (1998) The political science of risk perception. *Reliability Engineering & System Safety* 59(1): 91–99.

Jasanoff S (2004) (ed) *States of Knowledge: The Co-production of Science and the Social Order.* New York: Routledge.

Jasanoff S Kim S-H and Sperling S (2007) *Sociotechnical Imaginaries and Science and Technology Policy: A Cross-National Comparison*. NSF Research Project, Harvard University.

John G (2011) Freedom of information and transparency in Scotland: Disclosing persons as things and vice versa. *Anthropology Today* 27(3): 22–25.

Jolivette AJ (2015) *Research Justice: Methodologies for Social Change*, Bristol: Policy Press.

Jordan S, Mitterhofer H and Jørgensen L (2018) The interdiscursive appeal of risk matrices: collective symbols, flexibility normalism and the interplay of ‘risk’ and ‘uncertainty’. *Accounting, Organizations and Society* 67:4-55.

Kaun A and Treré E (2018) Repression, resistance and lifestyle: charting (dis)connection and activism in times of accelerated capitalism. *Social Movement Studies*. https://doi.org/10.1080/14742837.2018.1555752.

Kazansky B (2015) Privacy, responsibility, and human rights activism. *Fibreculture Journal* (26): 189–207. DOI: 10.15307/fcj.26.195.2015.

Kazansky B (2016) Digital Security in Context: Learning How Human Rights Defenders Adopt Digital Security Practices. Report, Tactical Tech, Berlin, Germany. Available at: https://cdn.ttc.io/s/secresearch.tacticaltech.org/pages/pdfs/original/DigitalSecurityInContext.pdf (accessed 21 May 2016).

Kazansky B, Torres G, van der Velden L, Wissenbach KR and Milan S (2019) Data for the social good: Toward a data-activist research agenda. In: A. Daly & M. Mann (eds.) *Good Data*. Amsterdam: Institute of Network Cultures.

Kazansky B (2021) ‘It depends on your threat model’: Understanding the anticipatory dimensions of resistance to data harms. *Big Data and Society* 8(1). https://doi.org/10.1177/2053951720985557

Kazansky B and Milan S (2021) “Bodies not templates”: Contesting dominant algorithmic imaginaries. *New Media & Society* 23: 363-381.

Kennedy H (2016) *Post, Mine, Repeat: Social Media Data Mining Becomes Ordinary*. New York: Springer.

Kennedy H, Poell T and van Dijck J (2015) Data and agency. *Big Data & Society* 2(2). https://doi.org/10.1177/2053951715621569.

Kennedy H (2018) Living with Data: Aligning Data Studies and Data Activism Through a Focus on Everyday Experiences of Datafication. *Krisis: Journal for Contemporary Philosophy*, 2018 (1): 18-30. ISSN 0168-275X

Law J (2004) *After method: Mess in social science research.* Abingdon: Routledge.

Lea J and Stenson K (2007) Security, Sovereignty, and Non-State Governance "from Below". *Canadian Journal of Law and Society* 22(2): 9-27.

Lehtiniemi T and Ruckenstein M (2018) The social imaginaries of data activism. *Big Data & Society*. DOI: 2053951718821146.

Leistert, O (2012) Resistance against cyber-surveillance within social movements and how surveillance adapts. *Surveillance & Society* 9(4): 441–456.

Lewis B (2013) *Facial Recognition Defense Workshop: A Make-Up Tutorial*. Available at: https://hankblog.wordpress.com/2013/04/09/facial-recognition-defense-work- shop-a-make-up-tutorial

Lewis T, Gangadharan SP, Saba M, Petty T (2018) *Digital defense playbook: Community power tools for reclaiming data.* Detroit: Our Data Bodies.

Li S, Trendacosta, K (2019) Shoot the messenger: How can we share secure messaging advice without causing harm? Available at: https://platform.internetInternetfreedomfestival.org/en/IFF2019/public/schedule/custom/1342 (accessed 25 April 2019).

L H (2020) A sociotechnical approach to cyber security. Report, National Cyber Security Centre, UK.

Lopez-Neira I, Patel T, Parkin S, et al. (n.d.) ‘Internet of Things’: How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly* 63: 22–26.

Lynn JW (2010) Defending a New Domain: The Pentagon’s Cyberstrategy *Foreign Affairs* 89(5):97–108;

Lyon D (ed) (2002) Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination. London and New York: Routledge

Lyon D (2014) Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society* 1(2). https://doi.org/10.1177/2053951714541861

Lyon D (2015) *Surveillance After Snowden*. Cambridge and Malden, MA: Polity Press.

Lyon D (2017) Surveillance culture: engagement, exposure, and ethics in digital modernity.
International Journal of Communication 11: 824–842.

Mackenzie A (2013) Programming subjects in the regime of anticipation: Software studies and subjectivity. *Subjectivity* 6(4): 391–405.

MacKenzie A (2017) *Machine Learners: Archeology of a Data Practice.* MIT Press, Cambridge, MA.

Mann S (2002) ‘‘Reflectionism’’ and ‘‘diffusionism’. In: Levin TY, Frohne U and Weibel P (eds) *CTRL [space]: Rhetorics of surveillance from Bentham to Big Brother.* Cambridge, Mass.: MIT Press

Mansell R (2012) *Imagining the Internet: Communication, Innovation, and Governance*. Oxford: Oxford University Press.

Marcus G (1998a) Ethnography in/of the world system: The emergence of multi-sited ethnography. In (ed. Marcus G) *Ethnography through thick and thin.* Princeton, NJ: Princeton University Press, pp.79-104.

Marcus G (1998b) Imagining the whole: Ethnography's contemporary efforts to situate itself. In (ed. Marcus G) Ethnography through thick and thin. Princeton, NJ: Princeton University Press, pp.33-56.

Marres N (2012) *Material Participation. Technology, the Environment and Everyday Publics*. Basingstoke, UK: Palgrave Macmillan.Mayer J (2013)

MakeUp Tutorial How to Hide from Cameras (n.d.) Available at: https://www.youtube.com/watch?v=kGGnnp43uNM (accessed 4 March 2018).

Martin A, Van Brakel R and Bernhard D (2009) Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. *Surveillance & Society* 6(3): 213-232.

Marwick, AE, boyd, d (2014) Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16(7): 1051–1067.

Marx GT (2009) A tack in the shoe and taking off the shoe: Neutralization and counter-neutralization dynamics. *Surveillance & Society* 6(3): 294–306.

Marx GT (2016) *Windows into the Soul: Surveillance and Society in an Age of High Technology.* Chicago: University of Chicago Press.

Maschmeyer L, Diebert R and Lindsay J (2020) A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics* 18(1): 1-20. DOI:10.1080/19331681.2020.1776658.

Massumi B (2015) *Ontopower: War, Powers, and the State of Perception*. Durham, NC; London: Duke University Press.

McCue C (2015) *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. 2nd edition. Oxford: Butterworth-Heinemann.

McInerney PB (2009) Technology movements and the politics of free/open source software. *Science, Technology, & Human Values* 34(2): 206–233.

Meyerson DE and Scully M (1995) Tempered radicalism and the politics of ambivalence and change. *Organization Science* 6: 585–600.

Milan S (2013) *Social Movements and Their Technologies: Wiring Social Change*. Basingstoke, UK: Palgrave Macmillan.

Milan S (2017) Data activism as the new frontier of media activism. In P. Victor, & G. Yang (eds.) *Media Activism in the Digital Age* (pp. 151-163). (Shaping Inquiry in Culture, Communication and Media Studies). London: Routledge.

Milan S (2018) Political agency, digital traces and bottom-up data practices. *International Journal of Communication* 12: 507–527.

Milan S and ten Oever N (2017) Coding and encoding rights in internetInternet infrastructure. *Internet Policy Review* 6(1). DOI: 10.14763/2017.1.442.

Milan S and Van der Velden L (2016) The alternative epistemologies of data activism. *Digital Culture & Society* 2(2): 57–74.

Millar K, Shires J and Tropina T (2021) Gender Approaches to Cybersecurity: Design, Defence and Response. Report, United Nations

Institute for Disarmament Research, Geneva, Switzerland. https://doi.org/10.37559/GEN/21/01

Miller A (2019) Shadows of war, traces of policing: The weaponization of space and the sensible in preemptionpreemption. In: Benjamin R (ed) *Captivating Technology: Race, Carceral Technoscience, and Liberatory Imagination in Everyday Life*. Durham: Duke University Press, pp. 85–106.

Miller L (2020) LAPD will end controversial program that aimed to predict where crimes would occur *Los Angeles Times,* 21 April.

Milner Y (2019) December 31. Abolition means the creation of something new. Available at: https://medium.com/@YESHICAN/abolition-means-the-creation-of-something-new-72fc67c8f493 (accessed 1 March 2021).

Minocher X and Randall C (2020 Predictable policing: New technology, old bias, and future resistance in big data surveillance. *Convergence: the international journal of research into new media technologies.* 26 (5-6): 1108-1124.

Mols AE and Pridmore JH (2019) When Citizens Are “Actually Doing Police Work”: The Blurring of Boundaries in WhatsApp Neighbourhood Crime Prevention Groups in The Netherlands. *Surveillance & Society 17* (3/4): 272-287. DOI: 10.24908/ss.v17i3/4.8664

Monahan T (2006) Counter-surveillance as political intervention? Social Semiotics 16(4): 515–534.

Monahan T (2010) Surveillance in the Time of Insecurity. Rutgers University Press.

Monahan T (2015) The Right to Hide? Anti-Surveillance Camouflage and the Aestheticization of Resistance. *Communication and Critical/Cultural Studies* 12(2): 159– 178.

Monsees L (2020) Cryptoparties: empowerment in internetInternet security? *Internet Policy Review* 9(4). https://doi.org/10.14763/2020.4.1508

Morgus R, Skierka I and Hohmann M (2015) National CSIRTs and Their Role in Computer Security Incident Response. Report, GPPI, Berlin, Germany. Available at: https://www.gppi.net/2015/11/19/national-csirts-and-their-role-in-computer-security-incident-response

Mouffe C (2013) *Agonistics: Thinking the World Politically.* London: Verso

Mueller M, Schmidt A and Kuerbis B (2013) Internet Security and Networked Governance in International Relations. *International Studies Review.* 15(1):86-104.

Mujinga M, Eloff M and Kroeze J (2017) A socio-technical approach to information security. In: Proceedings of the 23rd Americas Conference on Information Systems (AMCIS), Boston, MA, 10-12 August 2017 (pp. 1-10).

Murphy H and Bellamy M (2009) The Dazzling Zoologist: John Graham Kerr and the Early Development of Ship Camouflage. *The Northern Mariner/le marin du nord* XIX (2): 171–192.

Musiani F (2016) Alternative Technologies as Alternative Institutions: The Case of the Domain Name System. In: Musiani F, Cogburn DL, DeNardis L, et al. (eds) *The Turn to Infrastructure in Internet Governance*. Basingstoke, UK: Palgrave Macmillan, pp. 73–86.

Musiani F and Ermoshina K (2017) What is a good secure messaging tool? The EFF secure messaging scorecard and the shaping of digital (usable) security. *Westminster Papers in Communication and Culture* 12(3): 51–71.

Nissenbaum H (2005) Where computer security meets national security. *Ethics and Information Technology*, 7(2), 61–73. DOI: 10.1007/s10676-005-4582-3

Nissenbaum H (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life.* Stanford, CA: Stanford University Press.

Noble SU (2018) *Algorithms of Oppression: How Search Engines Reinforce Racism.* New York, NY: NYU Press.

Notley T and Hankey S (2013) Human Rights Defenders and the Right to Digital Privacy and Security in: *Human Rights and Information Communication Technologies: Trends and Consequences of use.* Hershey, PA: IGI Global.

O'Grady N (2016) A politics of redeployment: Malleable technologies and the localisation of anticipatory calculation. In: Louise, A, Piotukh, V (eds) *Algorithmic Life: Calculative Devices in the Age of Big Data*. Abingdon: Routledge, pp. 72–86.

O'Malley P (2010) Resilient subjects: uncertainty, warfare and liberalism. *Economy and Society* 39 (4): 488-509.

Parks L (2015) 'Stuff you can kick': Toward a theory of media infrastructure. In: Svens- son P and Goldberg DT (eds) *Between Humanities and the Digital*. Cambridge, MA and London, England: MIT Press, pp. 355–373.

Parrika, J (2007) *Digital Contagions – A Media Archaeology of Computer Viruses*. New York: Peter Lang.

Petty T, Saba M, Lewis T, Gangadharan SP and Eubanks V (2018) *Our Data Bodies: Reclaiming Our Data*. Detroit, MI: Our Data Bodies Project.

Pickett B (1996). *Foucault and the Politics of Resistance*. *Polity* 28(4), 445-466. DOI: 10.2307/3235341

Pink S, Lanzeni D, Horst H (2018) Data anxieties: Finding trust in everyday digital mess. *Big Data & Society* 5(1). DOI: 2053951718756685.

Polletta F (1999) 'Free spaces' in collective action. *Theory and Society* 28:1–38.

Power M (2007) *Organized uncertainty: Designing a world of risk management.* Oxford: Oxford University Press.

Power M (2009) The risk management of nothing. *Accounting, Organizations and Society*, 34(6/7): 849–855. DOI:10.1016/j.aos.2009.06.001.

Price R (2003) Transnational civil society and advocacy in world politics. *World Politics* 55(4): 579–606.

Puente M (2019) LAPD ends another data-driven crime program touted to target violent offenders. *Los Angeles Time*s 12 April.

Purdon L (2017) Cybersecurity should protect us – not control us. *Open Democracy,* 13 March 13. Available at: https://www.opendemocracy.net/en/digitaliberties/cybersecurity-should-protect-us-not-control-us/

Raghavan M, Barocas S, Kleinberg J (2020) Mitigating bias in algorithmic hiring: evaluating claims and practices. In Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency. Pp. 469-481.

Radloff J (2013) Digital Security as Feminist Practice. *Feminist Africa*. 18: 145–55.

Radloff J (2018) Embedding digital security in feminist movement building. Open Global Rights. Available at: https://www.openglobalrights.org/embedding-digital-security-in-feminist-movement-building/ (accessed 4 June 2020).

Reconfigure Network (2021) re: CONFIGURE. Feminist Action Research in Cybersecurity. Report, Oxford University, Oxford, UK. Available at:

https://www.oii.ox.ac.uk/wp-content/uploads/2021/01/Reconfigure-Report.pdf.

Reeves J (2012) If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility. S*urveillance & Society* 10(3/4): 235-248.

Rocha J (2021) A catalog of formats for digital discomfort… and other ways to resist totalitarian zoomification (eds) Gürses S and Rocha S (2021) available at: http://titipi.org/projects/discomfort/CatalogOFFDigitalDiscomfort.pdf

Rogers M and Eden G (2017) The Snowden disclosures, technical standards and the making of surveillance infrastructures. *International Journal of Communication* 11: 802–823.

Ruppert E (2018) Different Data Futures: An Experiment in Citizen Data. In: *DGINS* conference, Bucharest, 2018.
Ruppert E, Isin E and Bigo D (2017) Data Politics. *Big Data & Society* (July-December): 1–7. DOI: 10.1177/2053951717717749.

Rutkowska J (2011) The Invisible Things Lab's blog: Partitioning my digital life into security domains. In: *The Invisible Things Lab's blog*. Available at: https://theinvisiblethings.blogspot.com/2011/03/partitioning-my-digital-life-into.html (accessed 3 February 2018).

Rutkowska J and Wojtczuk R (2010) Qubes OS Architecture. Version 0.3. Invisible Things Lab.

Ryan-Mosley T and Strong J (2020) The activist dismantling racist police algorithms. MIT Technology Review.

Sassoon AS (2000) *Gramsci and Contemporary Politics: Beyond Pessimism of the Intellect.* London: Routledge.

Satchell C and Dourish P (2009) Beyond the user: use and non-use in HCI. *Human-Computer Interaction* 366: 9–16.

Schinkel W (2017) *Imagined Societies. A Critique of Immigrant Integration in Western Europe*. Cambridge: Cambridge University Press.

Schweitzer D (2003) How to toughen the weakest link in the security chain. *Computer world,* 8 January. Available at: https://www.computerworld.com/article/2580125/how-to-toughen-the-weakest-link-in-the-security-chain.html (accessed 21 May, 2021).

Scoones I and Stirling A (eds) (2020) *The politics of uncertainty: Challenges of transformation.* Routledge: Abingdon.

Shamas N (2017) Creating a pedagogy of empowerment. Available at: https://internetInternetfreedomfestival.org/wiki/index.php/Creating_a_pedagogy_of_empowerment (accessed 25 April 2019).

Shelton M (2018) Locking down signal: A guide for journalists. Available at: https://medium.com/@mshelton/locking-down-signal-d71678f653d3 (accessed 23 December 2020).

Shostack A (2014) Threat Modeling: Designing for Security. Indianapolis: Wiley.

Slayton R (2015) Measuring risk: computer security metrics, automation, and learning. *IEEE Annals of the History of Computing* 37 (2): 32-45.

Slayton R and Clarke B (2020) Trusting Infrastructure: The Emergence of Computer Security Incident Response, 1989–2005. *Technology and Culture* 61(1): 173-206.

Slupska, J (2019) Safe at Home: Towards a Feminist Critique of Cybersecurity. *St. Anthony's International Review* 15: 83-100. Whose

Security is Cybersecurity? Authority, Responsibility and Power in Cyberspace.

Sheehey, B (2019) Algorithmic paranoia: the temporal governmentality of predictive policing. *Ethics and InformationTechnology* 21(1): 49–58. https://doi.org/10.1007/s10676-018-9489-x

Shove E, Pantzar M and Watson M (2012) *The Dynamics of Social Practice: Everyday Life and How It Changes*. London: Sage.

Smith AM (2012) *Laclau and Mouffe. The Radical Democratic Imaginary*. London: Routledge.

Smith GJD (2018) Data doxa: The affective consequences of data practices. *Big Data and Society* 5(1): 1–15.

Snow DA, Worden S and Benford R (1997) Frame Alignment Processes, Micromobilization, and Movement Participation. In: McAdam D and Snow DA (eds) *Social Movements. Readings on Their Emergence, Mobilization, and Dynamics*. Los Angeles: Roxbury, pp. 235–251.

Stachowitsch S and Sachseder J (2019) The gendered and racialized politics of risk analysis. The case of Frontex. *Critical Studies on Security* 7(20):107-123.

Star SL (1999) The Ethnography of Infrastructure. *American Behavioral Scientist* 43(3): 377–391.

Star SL and Bowker GC (2007) Enacting silence: Residual categories as a challenge for ethics, information systems, and communication. *Ethics and Information Technology* 9(4): 273–280.

Star SL and Griesemer, J (1989) Institutional ecology, ‘translations,’ and boundary objects: Amateurs and professionals in Berkeley’s museum of vertebrate zoology. *Social Studies of Science* 19: 387–420.

Star SL and Ruhleder K (1996) Steps Toward an Ecology of Infrastructure: Design and Access for Large Information Spaces. I*nformation Systems Research*, 7(1): 111-134.

Stark L and Hoey J (2021) The ethics of emotion in AI systems. In FAccT'21: Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency, March 2021 (pp. 782–793). New York (NY): Association for Computing Machinery (ACM).

Stop LAPD Spying Coalition (2015) Architecture of Surveillance – Explained. Available at: https://stoplapdspying.org/policing-strategies-and-tactics/ (accessed 25 June 2020).

Stop LAPD Spying Coalition (2018) Before the Bullet Hits the Body — Dismantling Predictive Policing in Los Angeles. Report, Stop LAPD Spying Coalition, Los Angeles, CA. Available at: https://stoplapdspying.org/before-the-bullet-hits-the-body-dismantling-predictive-policing-in-los-angeles/ (accessed: 4 October 2019).

Stop LAPD Spying Coalition (2019a) Stop LAPD Spying Coalition Wins Groundbreaking Public Records Lawsuit. Available at: https://stoplapdspying.medium.com/stop-lapd-spying-coalition-wins-groundbreaking-public-records-lawsuit-32c3101d4575 (accessed: 6 April 2021).

Stop LAPD Spying Coalition (2019 b) The People's Response to OIG Audit of Data-Driven Policing. Available at: https://stoplapdspying.org/the-peoples-response-to-oig-audit-of-data-driven-policing (accessed: 25 June 2020).

Stop LAPD Spying Coalition and Free Radicals (2020) The Algorithmic Ecology: An Abolitionist Tool for Organizing Against Algorithms. Available at: https://medium.com/@stoplapdspying/the-algorithmic-ecology-an-abolitionist-tool-for-organizing-against-algorithms-14fcbd0e64d0 (accessed 3 April 2021).

Strathern M (2000) The tyranny of transparency. British Educational Research Journal 26(3): 309–321.

Suchman L (2002) Located accountabilities in technology production. *Scandinavian Journal of Information Systems* (14)2: 91-105. Available at:

Suchman L (2015) Situational awareness: Deadly bioconvergence at the boundaries of bodies and machines. *MediaTrope* 5(1): 1–24

Suchman L (2020) Algorithmic Warfare and the Reinvention of Accuracy In: Critical Studies on Security 8(2): 175-187. DOI: 10.1080/21624887.2020.1760587

Suchman L, Follis K and Weber J (2017) Tracking and Targeting: Sociotechnologies of (In)security. *Science, Technology, and Human Values* 42(6): 983-1002.

Swain V (2013) Disruption Policing: Surveillance and the Right to Protest. *Open Democracy,* 8 August. Available at: https://www.opendemocracy.net/en/opensecurity/disruption-policing-surveillance-and-right-to-protest (accessed 15 October 2020).

Tactical Tech Collective (2015) *Zen and the Art of Making Technology Work for You*. Available at: https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual (accessed 20 September 2018).

Tactical Technology Collective (2016) Holistic Security Manual. Available at: https://holistic-security.tacticaltech.org/ (accessed 20 September 2018).

Tactical Technology Collective (n.d.) Gendersec training curricula. Available at: https://xyz.informationactivism.org/en/ (accessed 20 September 2018).

Tactical Technology Collective (XYZ) (n.d.) Available at: https://xyz.informationactivism.org/en/ (accessed 22 February 2021).

Tanczer L, Lopez-Neira I, Parkin S et al. (2018). Gender and IoT Research Report: The Rise of the Internet of Things and Implications for Technology-Facilitated Abuse. Report, STEaPP, PETRAS IoT Hub, London.

Tanczer L, Deibert RJ, Bigo D, Franklin MI, Melgaço L, Lyon D, Kazansky B and Milan S (2020) Online Surveillance, Censorship, and Encryption in Academia. *International Studies Perspectives* 21(1): 1-36.

Tarnoff B (2020) The Making of the Tech Worker Movement. L*ogic Magazine,* 4 May. Available at: https://logicmag.io/the-making-of-the-tech-worker-movement/full-text/

Taylor L, Floridi L and van der Sloot B (eds) (2017) *Group Privacy: New Challenges of Data Technologies,* 1st ed. New York, NY: Springer.

The Citizen Lab (2014) Extended analysis: civil society perspectives and responses, from Communities @ Risk: Targeted Digital Threats Against Civil Society. Report, University of Toronto, Toronto. Available at: https://targetedthreats.net/media/2.3%20Extended%20Analysis-CivilSociety.pdf

The Engine Room (2013) Training digital security trainers: A preliminary review of methods, needs, and challenges. Report, The Engine Room for Internews, Washington DC, November.

The Engine Room (2018) Ties That Bind: Organisational Security for Civil Society. Report, The Engine Room for the Ford Foundation, New York, March.

Thomas DR (2003) A general inductive approach for qualitative data analysis. School of Population Health, University of Auckland, New Zealand.

Trottier D (2017) Digital Vigilantism as Weaponisation of Visibility. Philosophy of Technology 30: 55–72 https://doi.org/10.1007/s13347-016-0216-4

Tsing A (2015) *The Mushroom at the End of the World: on the Possibility of Life in Capitalist Ruins.* Princeton NJ: Princeton University Press.

Tufekci Z (2019) The Hong Kong Protesters Aren't Driven by Hope. *The Atlantic,* 12 November. Available at: https://www.theatlantic.com/international/archive/2019/11/escalating-violence-hong-kong-protests/601804/

Ullrich P and Knopp P (2018) Protesters' reactions to video surveillance of demonstrations: Counter-Moves, security cultures, and the spiral of surveillance and counter-surveillance. *Surveillance & Society* 16(2): 183–202.

Ulfstjerne MA (2020) BoB and the Blockchain: Anticipatory infrastructures of the cashless society. In *Who's cashing in? Contemporary perspectives on new monies and global cashlessness* (pp. 89-104). Berghahn Books.

Van Brakel R (2016) Preemptive big data surveillance and its (dis)empowering consequences: The case of predictive policing. In: van der Sloot B, Broeders D, Schrijvers E (eds) *Exploring the Boundaries of Big Data.* Amsterdam: Amsterdam University Press, pp. 117–141.

van der Velden L (2018) *Surveillance as public matter. Revisiting sousveillance through devices and leaks* (PhD dissertation). University of Amsterdam, The Netherlands.

van Dijck J (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197–208. https://doi.org/10.24908/ss.v12i2.4776

Van Dijck J, Poell T and De Waal M (2018) *The platform society. Public values in a connective world.* Oxford: Oxford University Press.

Veale M and Brown I (2020) Cybersecurity. *Internet Policy Review* 9(4) https://doi.org/10.14763/2020.4.1533

Verran H (1998) Re-imagining land ownership in Australia. *Postcolonial Studies* 1(2): 237–254.

Vertesi J (2014) Seamful Spaces Heterogeneous Infrastructures in Interaction. *Science, Technology, & Human Values* 39 (2): 264-84.

Wang, J (2018) *Carceral Capitalism.* Cambridge: The MIT Press.

Wash R and Rader E (2011) Influencing mental models of security: a research agenda. In Proceedings of the 2011 New Security Paradigms Workshop (NSPW '11). Association for Computing Machinery, New York, NY, USA, 57–66.

West SM (2017) Ambivalence in the (Private) Public Sphere: How Global Digital Activists Navigate Risk. In: *7th Workshop on Free and Open Communications on the Internet 17*, Vancouver, BC, 2017. USENIX Association.

Whitten A and Tygar JD (1999) Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In Proceedings of the 8th USENIX Security Symposium, pp. 169–183, Washington, DC, August 1999

Wood MA and Thompson C (2018) Crowdsourced Countersurveillance: A Countersurveillant Assemblage? *Surveillance & Society* 16(1): 20-38.

Woolgar S (1990) Configuring the user – The case of usability trials. In: Law, J (ed) *A Sociology of Monsters – Essays on Power, Technology and Domination*. London: Routledge, pp. 58–99.

Wyatt S (2003) Non-users also matter: The construction of users and non-users of the Internet In: Oudshoorn N and Pinch T (eds). *How users matter: The co-construction of users and technology.* Cambridge, Mass.: MIT Press, pp. 67–79.

Wyatt S (2004) Danger! Metaphors at work in economics, geophysiology, and the Internet. *Science, Technology & Human Values* 29(2): 242–261.

Zajko M (2018) Security against Surveillance: IT Security as Resistance to Pervasive Surveillance. Surveillance&Society16(1): 39-52.