UNIVERSITY OF AMSTERDAM

UvA-DARE (Digital Academic Repository)

What harms may come?

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

Kazansky, B.

Publication date
2021

Link to publication

Citation for published version (APA):
Kazansky, B. (2021). *What harms may come? Exploring the anticipatory dimensions of surveillance resistance in an age of datafication*. [Thesis, fully internal, Universiteit van Amsterdam].

General rights
It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations
If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please Ask the Library: https://uba.uva.nl/en/contact, or a letter to: Library of the University of Amsterdam, Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

UvA-DARE is a service provided by the library of the University of Amsterdam (https://dare.uva.nl)

Download date:23 Jan 2026

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