What harms may come?

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

Kazansky, B.

Publication date
2021

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).