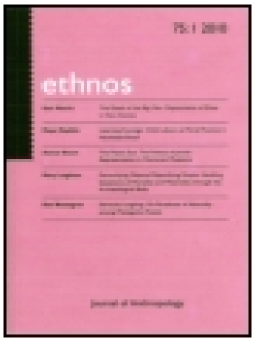

Routledge
Taylor & Francis Group

Ethnos
Journal of Anthropology

ISSN: 0014-1844 (Print) 1469-588X (Online) Journal homepage: https://www.tandfonline.com/loi/retn20

The Power to Selectively Reveal Oneself: Privacy Protection among Hacker-activists

Nina Dewi Horstmann

To cite this article: Nina Dewi Horstmann (2020): The Power to Selectively Reveal Oneself: Privacy Protection among Hacker-activists, Ethnos, DOI: 10.1080/00141844.2020.1721549

To link to this article: https://doi.org/10.1080/00141844.2020.1721549

Published online: 24 Mar 2020.

ETHNOS
https://doi.org/10.1080/00141844.2020.1721549

The Power to Selectively Reveal Oneself: Privacy Protection among Hacker-activists

Nina Dewi Horstmann

Department of Anthropology, Stanford University, Stanford, CA, USA

ABSTRACT

Privacy advocates and hacker activists ('hacktivists') oppose biometric technologies, such as electronic fingerprinting and facial recognition, that are increasingly used to sort and identify people. This paper draws from ethnographic fieldwork among technology experts and hacktivists in Denmark and Germany to explore how these individuals work to resist the encroachment of surveillance technologies in their physical and digital lives. Particular attention is paid to the practices they use to mask their locations, communications, and legal identities, thereby negotiating the border between public and private. This article describes how hacktivists exchange information about data protection and border-crossing to illustrate how encryption and other steps to protect privacy can be understood as moral practices. As opposed to common legal and philosophical definitions that characterise the right to privacy as inherent to the liberal, individual self, I suggest that hacktivists are advancing novel understandings of both identity and privacy as relational.

KEYWORDS hacking; surveillance; privacy; biometrics; Europe

> Privacy is the right to a self. Privacy is what gives you the ability to share with the world who you are on your own terms. For them to understand what you're trying to be and to protect for yourself the parts of you you're not sure about, that you're still experimenting with. If we don't have privacy, what we're losing is the ability to make mistakes, we're losing the ability to be ourselves.
>
> – Edward Snowden (quoted in Schrodt 2016)

The annual Chaos Communication Congress, hosted by Europe's largest collective of hackers, attracts over 10,000 technology and security enthusiasts with a 'critical-creative attitude towards technology' to code, build, drink, and debate the 'effects of technological advances on society' (CCC 2016). At the 2014 conference in Hamburg, a roguish, grinning hacker who goes by the name of 'starbug'[1] revealed how he reproduced the thumbprint of Ursula von der Leyen, the former German defence minister (CCC 2014). Dressed in a black hooded sweatshirt with the word 'Terrorist' written across his chest, starbug explained how he obtained von der Leyen's fingerprint from high-resolution photographs taken at a press conference and then used a commercial software

CONTACT Nina Dewi Horstmann ninadewi@stanford.edu

programme called Verifinger to map the print's ridges and whorls. He further demonstrated how one could make a 'dummy print' (a physical copy of an obtained fingerprint that can be used to fool biometric scanners) using household items like a laser printer, toner, and wood glue.

This hack was one of a number of starbug's stunts over the last decade – such as fooling the biometric readers used at the German passport office, breaking past Apple's TouchID, and publishing a politician's fingerprint lifted off a water glass – in which he and his colleagues publicly demonstrated the weaknesses of biometric systems as a form of political critique and activism (CCC 2013; 2017). His escapades have earned him widespread respect among the European hacker community, as well as notoriety among the politicians and corporations he has made an example of (see Grünenberg, this issue).

Biometrics refers to the measurement and recording of physical properties of the body, such as fingerprints, irises, and faces, which are then tethered to the legal identity of an individual. Biometric identification systems use sensors to scan biophysical characteristics and apply pattern recognition algorithms to convert unique bodily features into binary code. This code can then be stored within a database and/or transmitted across computer networks; in this way, 'bodies function as passwords' (Aas 2006). Nation-states are increasingly deploying biometric technologies for diverse purposes, such as border control, national ID cards, distribution of welfare benefits, law enforcement, and other instances that determine inclusion or exclusion from the national body. Following recent acts of terrorism and the 2015 'migration crisis', the rhetoric of securitisation has gripped Europe and liberal European states have adopted biometric technologies as tools to manage insecurity and uncertainty (Maguire *et al*. 2014). Meanwhile, biometric identification systems have also found applications in banking, commerce, mobile phones, and other personal electronics, often under the logic of enhancing security, as opposed to passwords or key-cards that can be forgotten or stolen. What starbug and his colleagues have revealed, however, is that biometrics can be duplicated and, therefore, are not nearly as secure as they purport to be. Biometric identifiers' uniqueness is also their liability; once a fingerprint or iris pattern has been compromised, it cannot be reassigned as easily as changing a password. While these technologies remain prone to ambiguity, inaccuracy, and technical failures (Magnet 2011), it is within these technical glitches that hackers locate possibilities for new forms of political critique and activism.

For hacker activists ('hacktivists'), hacking refers to playful, inventive and subversive technological activities that are often in front of or outside the law; hackers thus skirt the boundaries of both technical and legal possibility. Through their exploits, hacktivists work to expose security flaws and other problems that legal systems have yet to recognise. In addition to public-facing, curtain-raising hacks, they attempt to influence legislation and technological standards, encourage state transparency as they simultaneously advocate individual privacy, and raise public understanding of technological concepts (Postill 2018). In fact, members of the Chaos Communication Club have been asked to testify as expert witnesses in front of the German constitutional court, on topics such as government data retention and information security, on multiple occasions (Kubitschko 2015).

This article explores how hackers and privacy activists in Germany and Denmark engage in direct action to protect their communities against electronic surveillance; I will argue that, through their challenge of corporate and state surveillance, hacktivists offer a moral critique about protecting the collective. Through examining hacktivists' conceptions of identity and privacy, I demonstrate how they build upon and reconfigure existing legal definitions, thereby introducing new understandings of both identity and privacy as *relational*. Finally, I discuss how hacktivists exchange information about protecting one's privacy when travelling across borders. I suggest that border-crossing provokes anxiety among my informants, despite the European passports that provide them with freedom of mobility, because it is at the border that they confront state authority face-to-face, embodied in the figure of the border guard.

Methodology and Approach

The insights in this paper are based on fieldwork over a period of nine months among privacy advocates, hackers, activists, information security professionals, programmers, data protection lawyers, and digital artists in Denmark and Germany. Many of my informants occupy more than one of these aforementioned roles, often working professionally in information security or computer programming while pursuing activism in their personal time. During this period, I attended six hacker conferences and technology festivals, a number of privacy workshops and informal offline gatherings of technologists, and held over a dozen interviews. Following the pioneering work of other anthropologists and digital ethnographers (see Escobar *et al.* 1994; Coleman 2010), a portion of my fieldwork also took place online, particularly on Twitter and over encrypted email and chat messaging. Through participation and observation in online social networks, I began to understand the ways that hacktivists engage with the public and each other online, as well as the news stories, jokes, and images they share. I was also able to establish trust and make contacts that led to further online or in-person interviews. Following my informants' indications about the embeddedness of digital sociality within their everyday lived experience, I do not draw a strict distinction between online and offline activity in terms of analytic importance. While my ethnographic vignettes draw from in-person interactions, it is not my intention to exaggerate the significance of these offline meetings as opposed to fieldwork conducted online; I recognise cyber-sociality as meaningful and generative of new forms of social relationships and understandings of selfhood (Turkle 2005; Boellstorff 2008).

Previous scholars have commonly characterised hacker ethics in terms of liberal values of autonomy, self-determination, creativity, and individual expression (Levy 1984; Leach et al. 2009). I, too, found liberal discourses recurring throughout my fieldwork; privacy advocates and hacker activists often frame their critiques about the collection and storage of biometric information in terms of liberal concerns about privacy and informational self-determination as a human right for a free society.

However, as the anthropological literature on hacking has shown, hackers' ethics and politics cannot simply be reduced to textbook liberal ideals. In fact, Coleman and Golub (2008) offer hacking as a fertile site for exploring how liberalism (and its contradictions) are culturally articulated; they argue that liberalism can be understood as a cultural sensibility – rather than a coherent doctrine – that is expressed heterogeneously. Their work complicates not only our understanding of hacker morality, but of the liberal tradition at large, underscoring the need for new theories that account for points of contention *within* liberalism. In this article, I engage with Coleman and Golub's arguments by providing additional ethnographic insight into how hacktivists negotiate, reproduce, and reformulate liberal logics in practice.

Ethnographers have also noted the particular tension between (liberal) individualism and collectivism within the hacking community. For example, anthropologists Christopher Kelty (2008) and Gabriella Coleman (2013) have deftly illustrated how hackers balance communal values about sharing, reciprocity and mutual aid with individual desires to differentiate oneself for positive attention or profit. Coleman describes how hackers recognise the mutual benefit of collaboration and offer prodigious help to their peers while simultaneously relishing the recognition and personal satisfaction that comes from finding an ingenious solution that demonstrates their own unique talents. Kelty explores the legal and ethical questions about intellectual property and stewardship of common projects that arise among free and open source software developers, as well as how these individuals work to support collective rights by building various technical, social and legal infrastructures (see also Postill 2018 on teamwork and collaboration among nerd activists). On a slightly different tack, Marco Deseriis (2015) considers the case of Anonymous, a dynamic, amorphous organisation of Internet activists that repudiates the cult of heroic individualism that presumes a social movement must be led by a single identifiable leader by operating under a collective pseudonym. Deseriis argues that Anonymous' use of a shared pseudonym has important implications for how people think about themselves as individual and collective subjects. In a similar vein, in this article I will suggest that hacktivists in Denmark and Germany are putting forth new notions of identity and privacy that go beyond care of the discrete, liberal self.

Hacking, Anti-authoritarianism and Power

Hacktivists regard biometric technologies as part of a larger ecosystem of encroaching electronic surveillance on the part of state and corporate actors. Erik, a Danish security expert specialising in identity platforms, directed my attention to the underlying systems that work to locate, stabilise, and fix identities: 'Remember', he cautioned, 'it is the identification that kills. Biometrics is just the worst assault weapon … Biometric surveillance and collecting biometrics is hacking people. Much worse than hacking systems'. When Erik describes biometric surveillance as 'hacking people', he points to its goal of penetrating and capturing a subject's interiority through the inspection of bodily signs (Amoore and Hall 2009), a practice for which he reserves greater moral condemnation than hackers' infiltration of computer systems.

For hackers and privacy activists, biometric technologies shift between being regarded as both powerful and flawed, disturbing but also amusing in their failure or shortsightedness. Hacktivists frequently note the technologies' limitations and failures, yet they also regard surveillance, breaches, and intrusions of private life as something of an inevitability. As starbug explained to me in an interview over encrypted email:

> Those [EU biometric] databases, like all the others, are far from being safe. Just imagine how many people have access to them. And it's becoming even worse when other entities, such as various intelligence [agencies], are going to build and share their own. It's just a question of time [before] the biometric features of all the people in those databases will be hacked or leaked. Keep in mind how valuable those data already are or will become in the near future. I am sure you will be able to buy a large biometric dataset soon, like you can buy credit card numbers now.

Similarly, Erik offered his own pessimistic view: 'I have a harsh perception on data – if they can be abused, they will be abused. It's like natural resources. They are abused because some hold the ability to exercise power over others'. Digital rights activists and hackers therefore work to expose technical flaws and incompetencies in biometric systems as part of a larger anti-authoritarian political project that is deeply sceptical toward powerful actors and institutions (Jordan & Taylor 2004; Coleman 2017).

Through their repeated calls for decentralisation, hacktivists frame centralised power as the enemy – seen in the form of state authority and law enforcement, entrenched bureaucracies in the public and private sector, and monopolistic technology firms. Many hacktivists profess anti-fascist, leftist, and/or anarchist political leanings, an amalgamation that resembles the membership of other contemporary social movements in Europe – what Maple Razsa (2015) calls the 'uncivil society' of radical politics. Like other anti-authoritarian activists across the European continent, hacktivists engage in the principle of direct action, a method of enacting utopian ideals *through* alternative practices and innovative technologies (Juris 2008). For example, certain hacktivists work to create open-source tools that ensure privacy in an online landscape where users' data is increasingly collected and sold, or build online platforms, such as WikiLeaks, where incriminating information about state surveillance is exposed to the public.

Hacktivists' antipathy towards biometric technologies is situated within their broader critiques of diffused and normalised surveillance, the near-ubiquitous collection of personal data online, algorithmic profiling and prediction, the ascendance of Silicon Valley, high-profile data breaches, leaks revealing government misconduct, state-sponsored hacks, and the dizzying uptake of 'big data' solutions; all of which contribute to a fundamental reconfiguration of the relationships between the state, corporations, and individuals (see Deleuze 1992; Lyon 2003; Marx 2016). Within this broader landscape of electronic surveillance, biometric technologies are seen as especially pernicious because of the way that they blur the boundaries between the physical and the digital, as well as the public and the private. Notably, biometric sensors enable linkages between the physical body and data profiles based on past behaviour and/or predictive algorithms. As Stadler (2002: 120) describes, 'Our physical bodies are being shadowed by an increasingly comprehensive 'data body'. However, this shadow body does more than follow us. It does also precede us'.

Despite the escalation of state surveillance and 'surveillance capitalism' (Zuboff 2015), multiple privacy activists told me that one of their biggest challenges is making privacy perceptible as a socio-political problem, namely 'getting the average person to care'. These activists work under the premise that much of the public is nonchalant or wilfully participant in surveillance because 'regular people' believe they have 'nothing to hide'. What work does this narrative about surveillance and power do? This discourse tends to presume ambivalence, apathy, or ignorance on the part of the surveilled subject, rather than coerced cooperation or situations of non-consent. Further, in their enthusiasm to make their political message relevant to the broader public, privacy activists tend to sidestep how surveillance is a socio-political practice that often targets specific groups and populations (Dubrofsky & Magnet 2015; Hawthorne 2019). Similarly, power dynamics become oversimplified as a vulnerable public against a watchful ruling class. The universalist privacy discourse, so prevalent in hacktivist communities, therefore belies how mass surveillance is unevenly distributed and differentially experienced (Browne 2015).

When these hacktivists speak about surveillance, they tend to inexplicitly refer to the idealised liberal figure of the *private individual*: a law-abiding, rights-bearing citizen with a reasonable expectation of privacy. This is a particular sort of political subject, one much like themselves, a rational European citizen who faces the same surveillance threats and has the same capacity for reasoned deliberation and self-determination. Jean and John Comaroff (2012: 20) define this figure of the individual subject, as presented in liberal political philosophy, as 'an essentially Hegelian being, potentially capable everywhere of recognising, claiming, and affirming an unencumbered right to liberty on his or her own account, a being at once self-reflective, self-possessed, rationally self-motivated'. I argue that the presumption of rational and independent decision-making inherent to the figure of the liberal subject leads activists to overlook situations when surveillance is non-consensual or when the surveilled subject is considered to be outside the protections of the law (see Marx 2006).[2] However, in this article I will also show how hacktivists complicate the figure of the liberal, individual subject through their discourses and practices related to identity and privacy.

'Privacy is the Power to Selectively Reveal Oneself to the World'

We can draw a genealogy from the contemporary European hacker community to the legacy of the cypherpunks, an online movement that emerged in the 1990s. According to computer scientist Phillip Rogaway (2015: 17), 'the cypherpunks envisioned that one could hack power relations by writing the right code'. The cypherpunks created systems of encryption that allowed anonymous conversations and transactions to take place. Encryption is a method of encoding the contents of a message or file so that it can only be read by someone who holds the proper key. Cypherpunks believed in cryptography as a technical tool for protecting individual autonomy and privacy against the spectre of electronic surveillance. The 1993 *Cypherpunk Manifesto* by Eric Hughes, then a student at UC Berkeley, declared:

> Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world (Hughes 1993).

Privacy, for the cypherpunks, was therefore about control over the flow of data about oneself and the agency to determine who has access to personal information. European law reflects this liberal emphasis on individual decision-making through the principle of informational self-determination (*Informationsselbstbestimmung*). Like their cypherpunk forebears, contemporary hackers exercise their autonomy by modifying the flow of data about themselves; privacy activists encourage others to 'put static in the system' and fool algorithms that try to assemble profiles about users. When hacktivists disavow algorithms that attempt to calculate future behaviour based upon tendrils of data from one's past, they are asserting the individual's potential to change and behave unpredictably. In contrast to government and commercial attempts to capture, predict and stabilise identity, hacktivists understand identity as contextual, fluid and dynamic – what I refer to as identity as information versus identity as in-formation.

Identity as In-formation

In an interview in the *London Review of Books*, Craig Wright – cryptographer, computer scientist, and self-proclaimed inventor of Bitcoin[3] – mused, 'Where we are is a place where people can be private and part of that privacy is to be someone other than who they were. Computing will allow you to start again, if you want to. And that is freedom' (O'Hagan 2016). This claim echoes the sentiments of many hackers and privacy activists with whom I spoke that see the digital realm as an essential site for self-fashioning. According to these activists, privacy creates a space for personal expression to flourish, where one's identity can be cultivated. They argue that the experiments and alchemies that constitute the self deserve protection from external scrutiny.

Furthermore, they resist framings that regard masking or hiding in negative terms. As Marieke, a technologist and digital artist who employs different avatars online, told me, 'I don't believe in hiding but rather in living in a way that frees you from restrictive and identifiable bounds'. She continued, 'Using different faces gives me an opportunity to explore identity – it doesn't mean that you're hiding something'. When Marieke speaks of 'using different faces' in order to live freely from 'restrictive and identifiable bounds', she expresses a desire for liberation from a constrictive system that tethers one's face to expected behaviours. Rather than the negative connotations of deception and hiding, Marieke emphasises the productivity of masking for self-development.

The hacktivists I interviewed rejected the notion that anonymity or pseudonymity is about hiding a 'true' self; rather, they understand identity as multiple, contingent, and malleable. They explained to me how different aspects of the self are revealed, depending upon your social relationships with your audience: different 'faces' are shared with lovers, employers, family, acquaintances and friends. In this sense, these activists also gesture at how identity formation is intersubjective. By noting how different facets of the self are projected depending on social context, I suggest that these activists are arguing that our sense of self is always entangled with who we are in relation to others. Their comments point toward the fundamentally relational character of identity: namely, how self-cultivation is not only an individual project, but is accomplished through our relationships with other people (Jackson 2012). In the next sections, I will further explore how hacktivists expand ideas about the liberal, individual self through their conception of privacy as intersubjective and collective.

The Boundary Work of Privacy

Early in August of 2017, I arrived, excitable and diffident, in Bornholm, a sunny island of granite cliffs in the Baltic Sea. A small place, and relatively remote, it played home to an annual week-long hacker camp. Each year, clusters of colourful tents would spring up like wildflowers among the island's grassy fields and low, squat farmhouses. On my first night, I wandered through the campsite, in search of some action, and found a circlet of trees with several hammocks strung in their branches. A man was lounging horizontal in one of them, his laptop resting upon his stomach. Its screen reflected a soft bluish glow onto his face. Another man was selling local beers from behind a bar made of plywood and plastic sheeting. I bought one from him, handing over a fistful of the 3D-printed plastic tokens that were used as currency in the hacker camp. In search of a hammock of my own, I nearly tripped over a long orange cable that lay hidden in the grass like a snake. The hackers had set up a network of portable electric generators connected by a web of extension cords. Later, a DJ began to play a set and the forest was temporarily filled with blinking lights and thumping bass. People were starting to gather around the bar. I snapped a quick photo and uploaded it to Twitter, with the caption 'Live from the #BornHack bar'. With this picture and tagline, I meant to announce my presence, both to fellow attendees and those following the event vicariously online. Had I known then what I know now, I would have chosen differently.

Twenty minutes later, I received a message in my private inbox. It was Søren, an active member of the Danish hacker community, asking if I had requested the photo subjects' consent before taking the picture. He reminded me of the hacker camp's code of conduct, which stated to ask before filming. I explained that I hadn't thought about it, since the lighting was dark and the subjects' faces were completely in shadow; even the outline of their profiles was barely discernible against the blur of neon lights and the dark silhouettes of trees. My phone buzzed again. Søren replied that, given the high resolution of today's smartphones, one could never be too careful. He suggested deleting my post and taking a new photo, after asking for permission. As consolation, he offered to repost the new photo to his Twitter feed, which would give my photo publicity among his online followers.

Through his request, Søren expressed concern that fellow guests' privacy had been violated, since a photo of their faces and bodies, linked to a specific event and location, appeared online without their approval. He appealed to me to remove the photo in order to protect his friends and to maintain the privacy and sanctity of the hacker camp. By volunteering to repost my new photo, however, he also drew me closer into his online social network. In his strategy for enforcing privacy, he therefore fortified existing affective and social ties and built new ones (with myself). I interpret this interaction as an example of what sociologist Christena Nippert-Eng (2010) refers to as the 'boundary work' of privacy, namely the definition, enactment, management, and reinforcement of boundaries between the public and private.

Whereas philosophers and legal scholars have struggled to define what exactly constitutes privacy (Thomson 1975; Kahn 2003), I trace hacktivists' own understandings of privacy by focusing upon the work that they do to construct a border between their private and public lives. Hacktivists draw upon both social and technical means to mask their locations, communications, and legal identities, thereby negotiating the border between public and private, exterior and interior. By looking at hacktivists' practices of boundary work, we can glimpse the instability of the border between public/private, which is constantly (re)drawn and/or maintained by individuals in their daily lives (Landes 1998; Cohen 2012). By referring to hacktivists' practices as boundary *work*, I also want to underscore the laborious nature of their techniques, which are often difficult to set up and adhere to, and which create added inconvenience and friction in everyday communications and online activity. Such technical practices include the use of encrypted emails, alternative chat programmes, and anonymous browsing software. Additionally, hackers' use of irony, sarcasm, elusiveness and pseudonymity can be understood as a social method of privacy management (Coleman 2015). As I learned from Andrey, a Russian national and long-time resident of Berlin, he tries to 'enforce end-to-end encryption not because [he is] communicating about anything secretive but to flood network traffic' with unreadable data. Andrey characterised his own practices as 'productive paranoia', self-ironically recognising that they may seem excessive, yet justifying his suspicion and mistrust by pointing to known cases of government and corporate intrusions.

Privacy as Moral Practice

Certain privacy activists and security experts work to transfer knowledge about digital protection through events called CryptoParties, where amateurs and enthusiasts explore the principles and practices of encryption, anonymity, and information security. The CryptoParty website (2018) explains the rationale for these events, hosted around the world but mostly clustered in Western Europe: 'Privacy is the space in which ideas are developed, to retreat into whenever you want. This space is not only physical but digital as well. Governments and companies don't want to respect that, so we become active ourselves'. Through attending CryptoParties, I was able to discuss security concerns with privacy activists, observe how information about encryption tools and surveillance threats is circulated, and learn how they negotiate and enact anonymity in practice. As I will demonstrate in this section, through these technologies of encryption, notions about the private, the individual, and the communal are being challenged and taking new forms.

In the absence of strong legal protections, safeguarding privacy has become framed as a personal responsibility and a moral imperative, characterised by self-restraint. As Fabian, a 'CryptoParty angel' (as volunteer instructors are called) told me, 'The fastest way to protect yourself is by changing your [own] behaviour'. Recommendations about selecting passwords or protection of electronic devices when crossing borders are thus offered with strong moral overtones. At a May 2017 CryptoParty held in a neon-lit hackerspace in East Berlin, Fabian asked me what I planned to do with the files on my computer when I returned to the United States. He knew that I had been conducting interviews and writing field notes about my interactions with hackers. How did I intend to protect that information when crossing the border?

Fabian helped me set up an encrypted partition on a USB flash drive and suggested that I mail the USB stick to my U.S. address rather than carrying it on the plane. He also advised me about selecting a strong password, dissuading me from including any sort of personal or anecdotal information. Security experts are critical of the way that many individuals insert their memories, sentimental attachments, and identities into their passwords. Instead, he presented me with a set of six ordinary plastic dice and a phrasebook for turning randomly generated numbers into words. Through rolling dice, one is able to generate sufficient randomness, or 'entropy', which a password selected on the basis of personal associations lacks. Fabian looked away carefully as I rolled the dice seven times in a row. Once my 42-character-long password, made up of a random and easily forgettable succession of words, was complete and scrawled on an index card, he described the memory games he repeats each morning in order to retain such complex password phrases. Hackers and privacy activists encourage people to improve their own 'digital hygiene' as an initial step toward protecting the rest of their social network; one supports the common cause through individual self-responsibility. Liberal conceptions about self-determination therefore underlie and enable this particular kind of activist practice.

At CryptoParties, the advice that is offered is saturated with moral prescriptions of how one ought to behave; duties of protection, self-surveillance, and privacy are inflected with an almost puritanical character. Indeed, the emic term 'angel' used to describe volunteer instructors invokes gratitude for their dedication and generosity, but also a sense of their moral authority. Morality, however, is not only about practices of self-comportment or discipline but is also about compassionate relations towards others. While waiting for my computer to finish generating an encrypted folder, I asked another volunteer 'angel' why she became involved in CryptoParties. She paused, biting her lip, and explained her motivations in terms of moral obligation: 'With everything going right now [politically], I felt like I had to do something to help'. The rituals of password creation and memorisation, as well as encryption, described by the CryptoParty activists are marked with moral claims about the proper way of acting and being – in order to not only protect one's self, but also the lives of others who our communications and personal data are intrinsically imbricated with. For example, in the case of email or chat programmes, communication by its nature involves two or more people, as well as any others about whom the message might refer.

By looking at privacy and secrecy as practices that do more than just conceal, I began to understand privacy as not only about protecting the bounded self. I started to see how practices of cloaking and encryption create an environment for intimate connections and trust to develop and be sustained. We can therefore think about privacy as an inherently social practice (Reiman 1976). Moving beyond an analysis of individual privacy and personal data also shows us how hackers work to fulfil a moral obligation of protecting their personal networks and communities, particularly those who are less technologically adept.[4] Rather than simply protecting themselves as atomised individuals, hacktivists understand their data as social and relational[5], constituted through interactions with others.

Hacktivist practices reveal an understanding of the individual self as irreducible from one's broader social relationships. As Jens, a Danish IT lawyer and privacy activist, wondered aloud to me, 'What does it mean to say *my* data? Data is socially produced. We produce data when interacting with each other and that is embedded in institutions'. Through this comment, Jens gestures at how data is borne of shared experiences and interactions, while also noting how these exchanges often occur on corporate platforms or intersect with the purview of government institutions.

I suggest that hacktivists have introduced a profound understanding of collective privacy that is not simply the aggregate of the privacy rights of discrete individuals; it is more than the sum of its parts. Rather, collective privacy supports the cultivation and maintenance of intersubjective relations between individuals, as well as the integrity of the group as a whole. Indeed, anthropologists have demonstrated how privacy and secrecy are generative for building social bonds, community, shared identities, intimacy, and trust (Simmel 1906; Jones 2014; Manderson *et al.* 2015). In championing a notion of privacy that extends beyond the individual self, hacktivists recognise the porousness between the self and trusted partners while still defending a hardened outer rind of protection against intrusions.

Protecting Privacy at the Border

At the 2017 Chaos Communication Congress, a queue had formed outside of the lecture hall, snaking its way down the stairs of the Leipziger Messe convention centre. Anticipation hung in the air like a garland. Hundreds of hackers had lined up to hear a lecture on 'Protecting Your Privacy at the Border', led by two activists from the Electronic Frontier Foundation (EFF). The presentation discussed the legal aspects of border searches, recent changes in travel and immigration policies, and the rights of border crossers to refuse digital search and seizure. Standing in the queue, I ran into Carsten, an affable young Danish hacker who I had kept in touch with after we met at a previous hacking convention. As we waited, we traded stories about other hackers and activists who had been detained, arrested, and/or charged with obstruction at European and American borders for refusing to unlock encrypted devices or turn over their passwords. Several of the stories he proffered I had heard before, though the narrative details varied slightly in each retelling; these stories circulated with the liveliness of an urban legend.[6] Trading border-crossing stories was a way to spread information in a context where one might be suspicious of official reports. It was also a way to demonstrate protective care, a reminder to remain vigilant under the watchful eye of state surveillance. As Sarah Luna (2018) has described in her work among sex workers living in the midst of military and narco-violence in Reynosa, Mexico, these types of rumours function as political critiques, at the same time as they work to strengthen social and protective bonds among storytellers and listeners. Sharing such stories brings the storyteller and the listener together as collective subjects: we, who are being targeted; we, who are in danger.

Why is border-crossing such a concern for hackers and technologists with relatively high income and education levels, as well as (mostly) European passports? Despite the mobility and socio-economic privilege granted by their European citizenship, the border still represents a point of friction for these hacktivists, where the state is granted extraordinary powers to capture intrusive data and demand personal information. Privacy activists therefore trade information and tips about how one can limit the collection of personal data, disable the RFID chips in biometric passports, and safely pass through borders without having their electronic devices searched. Because inspections of electronic devices may expose personal as well as relational data, border searches are a threat not only to individual privacy, but also to collective privacy. These activists are especially aware of the fact that at the U.S. border, one can be compelled to biometrically unlock their mobile phone, because, while passwords are covered by 5th Amendment protections against self-incrimination, biometrics are not.[7]

Border-crossing functions as an event – a moment of rupture, an extraordinary break from routine – that makes contradictions plain and exposes the true order of things. At the territorial border, hacktivists' political ideals and their moral imperative to protect their relational and personal data are tested. As Mark Salter (2008) has cogently argued, the border provokes ontological insecurity and a 'confessionary complex', even among lawful citizens, by forcing them to account for their travel and their possessions. By requiring individuals to declare their intentions (such as on customs forms or at checkpoints), as well as hand their belongings and bodies over for state scrutiny, even documented citizens are treated as suspicious at the border (see Møhl, this issue). Travellers' physical bodies and digital selves are also collapsed at border checkpoints, where biometric information is collected, data profiles are assembled and crosschecked, and electronic devices are inspected. Hacktivists therefore plan ahead by encrypting their devices, refraining from transporting electronics across borders, carrying dummy devices or air-gapped computers that have never been connected to the Internet, or sending devices ahead of time through the postal mail (where they are less likely to be inspected by border guards).

At the CCC event, hackers' anxieties about border-crossing were fuelled by information relayed by the EFF activists, who shared that electronic media searches at the U.S. border increased by 500% from 2015 to 2016, though the odds of having one's devices searched remains low (Opsahl & Budington 2017). Additionally, hackers likely imagine themselves to be at greater risk for border searches than the average person because of the way that hacking has become harshly criminalised in both the

United States and Western Europe. Helen Nissenbaum has tracked the shift in public perception of hackers, first seen as quirky programming enthusiasts but now popularly imagined as cyber-villains. According to Nissenbaum (2004: 209), law enforcement and the media have normatively reframed hackers because of the threat they pose to centralised authorities: 'established institutions have tried to increase the distance between hackers and the rest of us by means of an ontological transformation that reconceives hackers as deviants, and hence fair targets for repression and punitive action'. Yet, hackers like starbug appeal to and reproduce popular stereotypes about their extraordinary ability to manipulate computer systems within their political activism, thereby contributing to their own criminalisation and mystique. Within a society that values technical knowledge, hackers are respected for their expertise, even as they may be feared for their mischievous intentions. Because hackers' authority is derived from their ability to subvert the system, they occupy a certain figural space in the imaginations of biometric developers, governments, and the public (see Grünenberg, this issue).

Hackers, whose domain of authority, invention, and resistance is the digital realm, must present their physical bodies and electronic devices for inspection when crossing the border. At the border they come into direct, visceral contact with state power, as their fingertips touch the glass of biometric scanners or as their bodies are patted down by a border guard. They thus imagine the border as an affective site of anxiety and privacy loss, where EFF activists claim, 'many countries will conduct more invasive searches than their constitutions would otherwise allow' (Opsahl & Budington 2017). I suggest this anxiety emerges because the limits of liberal citizenship present themselves at the border. These tensions become meaningful against the backdrop of hacker politics' anti-authoritarianism and the punitive criminalisation of hacking. Potential infringements on civil liberties when crossing the border present a challenge to rights-based discourses that refer to the liberal democratic state as the guarantor of human rights. I point out these contradictions not to invalidate hacktivists' political struggles and claims, but to direct attention to the ways they reckon with these ambiguities and draw upon liberal sensibilities and language when expressing their disquietude: for example by characterising border searches as an 'affront to privacy and dignity which is inconsistent with the values of a free society' (Opsahl & Budington 2017).

Conclusion

In this article, I have examined the 'right to privacy' as both an analytical framework for understanding how privacy constitutes (individual and collective) subjectivity and as a political ideal around which direct action, civil disobedience and hacktivism congeal. In their fight for privacy, hacktivists assert the right of the individual to determine, develop and define their own identity; privacy is framed as the basis for liberty, dignity, personhood, and democracy. I have described the prevalence of liberal discourses within hacktivism and discussed how the figure of the liberal subject contributes to a specific, partial view of surveillance and power. However, I also note the tension between hacker liberalism and anti-authoritarianism, which is laid bare at the border, where invasive searches and seizures reveal the limitations of the state as the guarantor of liberal freedoms and human rights. Finally, I illustrate how hacktivists reconfigure liberal logics about the private, individual self through their conceptions of privacy and identity as relational. By pointing to the collective importance of privacy, their insights disrupt legal definitions that presume the right to privacy inheres within the liberal self, as well as push scholars to rethink theories that emphasise the individuating aspects of biometrics and surveillance technologies (Lyon 2003; Magnet 2011).

While others in this special issue have introduced how biometric technologies influence questions of membership and belonging within the national body, this article shows how hackers are pioneering new modes of political inclusion through hacking as critique. Within technical failures, hacktivists locate new sites of political intervention and possibility; they detect vulnerabilities in both technical systems and political structures, exploit malfunctions, introduce glitches, and cause breakdowns as a form of resistance and refusal. Biometric identification systems therefore do not straightforwardly infringe upon privacy, they have also generated novel forms of political participation and collective action on the part of hacktivists.

Finally, this article has explored the technical and social practices around which hacktivists' moral community is organised. I have argued that hackers' concerns for privacy are borne out of feelings of intersubjective ethical responsibility, solidarity, and commitment to their communities in the face of persistent and pervasive surveillance. Reading encryption as a moral practice allows us to appreciate the subtle, everyday gestures of care that occur between hacktivists and their larger social networks. In relation to this, I have demonstrated how hacktivists expanded the notion of privacy to include the protection of collective togetherness. In 2018, at the time this article was written, media attention about data breaches and the collective-level social harms caused by these privacy intrusions made hacktivists' activities even more salient. In this regard, I understand hacktivism as a powerful and cogent critique against modes of sorting, objectifying and identifying people. From hacker activists in Germany, Denmark and beyond, we can learn about how people strive to protect themselves, and those they live with, against powers they perceive as predatory in new digital terrains.

Notes

1. Given the heightened privacy concerns of my informants, all names are pseudonyms –except in the case of publicly identified hacks – and biographical details are brief to ensure anonymity.
2. Privacy activists often proffer technical services to journalists, activists, and human rights defenders – groups they have identified as particularly vulnerable to surveillance based on professional or political affiliation. However, they less frequently characterise surveillance as a practice that affects certain groups based upon race, nationality/citizenship status, sexuality, gender, or class. Hacktivists repeatedly emphasise how *everyone* should be concerned about surveillance because *everyone* has the right to a private life. This is unsurprising when considering the popular cultural imagination of the unmarked liberal subject. Yet, even as liberal rhetoric purports to promote and protect 'universal' freedoms, various scholars have demonstrated how European liberalism has historically (Arendt 1973; Mehta 1999) and contemporarily (Fernando 2014; Mahmud 2014) relied upon the political and social exclusion of certain groups of people.

3. The person(s) responsible for the development of Bitcoin employed the pseudonym Satoshi Nakamoto; their true identity remains unknown. Craig Wright is one of several individuals who has been linked with Bitcoin and perhaps the most vocal claimant. However, his claim is disputed by multiple developers and journalists. I find Wright's comments about privacy and the potential to re-invent the self to be intriguing precisely because of his embroilment in this controversy.
4. This can also be observed in hacktivist practices such as the construction of community Internet networks that employ decentralised mesh networks and VPN tunnels to bolster confidentiality (see De Filippi & Tréguer 2015), like Berlin's Freifunk, which has provided free wireless connections to dozens of refugee shelters in Germany.
5. While most biometric identifiers pertain only to an individual, DNA is a type of personal data that inherently relates to, and in certain contexts implicates, biological family members. See Suter 2010 and Olwig, this issue, for discussion of how familial DNA is used by the state to identify individuals and/or establish biological relationships for criminology and family reunification purposes.
6. By calling these stories 'rumours', I do not mean to imply that they are untrue or unfounded; I recognise that they are based off the cases of actual persons. However, I follow Luna (2018: 64) and other scholars of rumour in that I am less concerned with 'the veracity of narratives but rather examine them to make sense of particular political conditions.' In the case of hacker arrests, I am intrigued by how certain figures have taken on an outsized, almost mythological importance and their stories are told as cautionary tales.
7. Erin Sales (2014: 222) explains, 'the Supreme Court has repeatedly held that compelling an accused to demonstrate physical characteristics for identification purposes does not qualify as compelled self-incrimination because it is not testimonial in nature.'

Acknowledgements

This work was supported by the Yale Fox International Fellowship and grants from the Yale Center for Race, Indigeneity and Transnational Migration and the Stanford Center on Philanthropy and Civil Society. I extend my appreciation to the two reviewers for this journal, Duana Fullwiley, Miyako Inoue, Mathias Levi Toft Kristiansen, Margaux Fitoussi, the members of the Biometric Borderworlds research group, and the participants of the Stanford Anthropology Department Brown Bag Seminar and the Stanford Graduate STS Workshop for their valuable feedback at various stages of this article.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

ORCID

Nina Dewi Horstmann http://orcid.org/0000-0003-3937-1215

References

Aas, K. F. 2006. 'The Body Does Not Lie': Identity, Risk and Trust in Technoculture. *Crime, Media, Culture*, 2(2):143–158.

Amoore, Louise & Alexandra Hall. 2009. Taking People Apart: Digitised Dissection and the Body at the Border. *Environment and Planning D: Society and Space*, 27(3):444–464.

Arendt, Hannah. 1973. *The Origins of Totalitarianism* (New ed.). New York, NY: Harcourt Brace Jovanovich.

Boellstorff, Tom. 2008. *Coming of Age in Second Life: An Anthropologist Explores the Virtually Human*. Princeton: Princeton University Press.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press.

CCC. 2013. Chaos Computer Club Hackt Apple TouchID. Chaos Computer Club. https://www.ccc.de/updates/2013/ccc-breaks-apple-touchid (Accessed 21 September 2013).

———. 2014. *Ich sehe, also bin ich … Du: Gefahren von Kameras für (biometrische) Authentifizierungsverfahren*. Hamburg. https://media.ccc.de/v/31c3_-_6450_-_de_-_saal_1_-_201412272030_-_ich_sehe_also_bin_ich_du_-_starbug.

———. 2016. 33C3 Main Page. Chaos Computer Club. https://events.ccc.de/congress/2016/wiki/Main_Page (Accessed 27 December 2016).

———. 2017. Heute Mal Ohne Biometrie: Reisepass "well Done". Chaos Computer Club. https://www.ccc.de/en/updates/2017/chip-zappen (Accessed 7 April 2017).

Cohen, Julie. 2012. What Privacy Is For. *Harvard Law Review*, 126(7):1904–1933.

Coleman, E. Gabriella. 2010. Ethnographic Approaches to Digital Media. *Annual Review of Anthropology*, 39(1):487–505.

———. 2013. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press.

———. 2015. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Bloomsbury.

———. 2017. From Internet Farming to Weapons of the Geek. *Current Anthropology*, 58(S15):S91–S102.

Coleman, E. Gabriella & Alex Golub. 2008. Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism. *Anthropological Theory*, 8 (3):255–277.

Comaroff, Jean & John L. Comaroff. 2012. *Theory From the South: Or, How Euro-America Is Evolving Toward Africa*. Boulder: Paradigm Publ.

CryptoParty. 2018. What Is a CryptoParty? https://www.cryptoparty.in/ (Accessed 11 January 2018).

De Filippi, Primavera & Félix Tréguer. 2015. Expanding the Internet Commons: The Subversive Potential of Wireless Community Networks. *Journal of Peer Production* (6):1–40.

Deleuze, Gilles. 1992. Postscript on the Societies of Control. *October* 59: 3–7.

Deseriis, Marco. 2015. *Improper Names: Collective Pseudonyms From the Luddites to Anonymous*. Minneapolis: University of Minnesota Press.

Dubrofsky, Rachel E. & Shoshana Magnet (eds). 2015. *Feminist Surveillance Studies*. Durham: Duke University Press.

Escobar, Arturo, David Hess, Isabel Licha, Will Sibley, Marilyn Strathern & Judith Sutz. 1994. Welcome to Cyberia: Notes on the Anthropology of Cyberculture. *Current Anthropology*, 35(3):211–231.

Fernando, Mayanthi. 2014. *The Republic Unsettled: Muslim French and the Contradictions of Secularism*. Durham: Duke University Press.

Hawthorne, Camilla. 2019. Dangerous Networks: Internet Regulations as Racial Border Control in Italy. In *DigitalSTS: A Field Guide for Science & Technology Studies*, edited by J. Vertesiet al., 178–197. Princeton, NJ: Princeton University Press.

Hughes, Eric. 1993. A Cypherpunk's Manifesto. https://www.activism.net/cypherpunk/manifesto.html (Accessed 9 March 1993).

Jackson, Michael. 2012. *Between One and One Another*. Berkeley: University of California Press.

Jones, Graham M. 2014. Secrecy. *Annual Review of Anthropology*, 43(1):53–69.

Jordan, Tim & Paul A. Taylor. 2004. *Hacktivism and Cyberwars: Rebels with a Cause?* London: Routledge.

Juris, Jeffrey S. 2008. *Networking Futures: The Movements Against Corporate Globalization*. Experimental Futures. Durham: Duke University Press.

Kahn, Jonathan. 2003. Privacy as a Legal Principle of Identity Maintenance. *Seton Hall Law Review*, 33 (2):371–410.

Kelty, Christopher M. 2008. *Two Bits: The Cultural Significance of Free Software*. Durham: Duke University Press.

Kubitschko, Sebastian. 2015. Hackers' Media Practices: Demonstrating and Articulating Expertise as Interlocking Arrangements. *Convergence: The International Journal of Research Into New Media Technologies*, 21(3):388–402.

Landes, Joan B. (ed). 1998. *Feminism, the Public and the Private*. Oxford: Oxford University Press.

Leach, James, Dawn Nafus & Bernhard Krieger. 2009. Freedom Imagined: Morality and Aesthetics in Open Source Software Design. *Ethnos*, 74(1):51–71.

Levy, Steven. 1984. *Hackers: Heroes of the Computer Revolution*. Garden City, N.Y: Anchor Press/ Doubleday.

Luna, Sarah. 2018. Affective Atmospheres of Terror on the Mexico–U.S. Border: Rumors of Violence in Reynosa's Prostitution Zone. *Cultural Anthropology*, 33(1):59–84.

Lyon, David (ed). 2003. *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge.

Magnet, Shoshana. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham: Duke University Press.

Maguire, Mark, Catarina Frois & Nils Zurawski (ed). 2014. *The Anthropology of Security: Perspectives From the Frontline of Policing, Counter-Terrorism and Border Control*. London: Pluto Press.

Mahmud, Lilith. 2014. *The Brotherhood of Freemason Sisters: Gender, Secrecy, and Fraternity in Italian Masonic Lodges*. Chicago: The University of Chicago Press.

Manderson, Lenore, Mark Davis, Chip Colwell & Tanja Ahlin. 2015. On Secrecy, Disclosure, the Public, and the Private in Anthropology. *Current Anthropology*, 56(S12):S183–S190.

Marx, Gary. 2006. Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information. In *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by Torin Monahan, 37–56. Portland: Wilan.

———. 2016. *Windows Into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: University of Chicago Press.

Mehta, Uday Singh. 1999. *Liberalism and Empire: A Study in Nineteenth-Century British Liberal Thought*. Chicago: University of Chicago Press.

Nippert-Eng, Christena. 2010. *Islands of Privacy*. Chicago: University of Chicago Press.

Nissenbaum, Helen. 2004. Hackers and the Contested Ontology of Cyberspace. *New Media & Society*, 6 (2):195–217.

O'Hagan, Andrew. 2016. The Satoshi Affair. *The London Review of Books*, June 2016.

Opsahl, Kurt & William Budington. 2017. Protecting Your Privacy at the Border: Traveling with Digital Devices in the Golden Age of Surveillance. Presented at the 34th Chaos Communication Congress, Leipzig, Germany, December 29. https://events.ccc.de/congress/2017/Fahrplan/events/9086.html.

Postill, John. 2018. *The Rise of Nerd Politics: Digital Activism and Political Change*. Anthropology, Culture & Society. London: Pluto Press.

Razsa, Maple. 2015. *Bastards of Utopia: Living Radical Politics After Socialism*. Bloomington: Indiana University Press.

Reiman, Jeffrey. 1976. Privacy, Intimacy, and Personhood. *Philosophy & Public Affairs*, 6 (1):26–44.

Rogaway, Phillip. 2015. The Moral Character of Cryptographic Work. *IACR Distinguished Lecture*. Auckland, New Zealand.

Sales, Erin M. 2014. The Biometric Revolution: An Erosion of the Fifth Amendment Privilege to Be Free From Self-Incrimination. *University of Miami Law Review*, 69(1):193–240.

Salter, Mark B. 2008. When the Exception Becomes the Rule: Borders, Sovereignty, and Citizenship. *Citizenship Studies*, 12(4):365–380.

Schrodt, Paul. 2016. Edward Snowden Just Made an Impassioned Argument for Why Privacy Is the Most Important Right. *Business Insider*, September 15, 2016. http://www.businessinsider.com/edward-snowden-privacy-argument-2016-9.

Simmel, Georg. 1906. The Sociology of Secrecy and of Secret Societies. *American Journal of Sociology*, 11(4):441–498.

Stadler, Felix. 2002. Opinion: Privacy Is Not the Antidote to Surveillance. *Surveillance & Society*, 1 (1):120–124.

Suter, Sonia M. 2010. All in the Family: Privacy and DNA Familial Searching. *Harvard Journal of Law & Technology*, 23(2):310–399.

Thomson, Judith Jarvis. 1975. The Right to Privacy. *Philosophy & Public Affairs*, 4 (4):295–314.

Turkle, Sherry. 2005. *The Second Self: Computers and the Human Spirit*. Cambridge: MIT Press.

Zuboff, Shoshana. 2015. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30(1):75–89.