2015 | *Hau: Journal of Ethnographic Theory* 5 (2): 383–390

BOOK SYMPOSIUM

Edgework, state power, and hacktivists

Adam Fish and Luca Follis, *Lancaster University*

Comment on Coleman, Gabriella. 2014. *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. London and New York: Verso.

In *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous* (2014), Gabriella Coleman tracks the emergence of Anonymous from individual trollers to a "living network" of effective hacktivists (Thacker 2004). Anonymous has been both lionized and demonized but always mythologized to the point of obfuscation. The identities of individuals within Anonymous are complex and paradoxical: a mix of technological determinism and autonomy, social liberalism and libertarianism, individualism and collectivism, order and chaos. These themes extend from Coleman's earlier work on the pleasures of free and open source computing (Coleman 2012) and the technoliberal political identities of hackers (Coleman and Golub 2008). The book accomplishes a rare methodological feat: it makes it possible to believe that powerful, secretive individuals are not impossible to ethnographically research and that rapport can develop in spaces where trust is unlikely.

HHWS provides a valuable glimpse into hacker practice and identity; humanizing Anonymous while revealing the characters behind the Guy Fawkes mask, but it also offers a window into their criminal investigation, prosecution, and eventual incarceration. Indeed, somewhat unexpectedly, the state is a looming presence throughout the book. As the movement grows bolder and more confident, the US government (in its varied corporate, penal, security, and military guises) becomes an increasingly frequent target of Anonymous activism (e.g., #FuckFBIFridays, #ShootingSherrifsSaturday, #MilitaryMeltdownMonday). At the same time, visits from law enforcement become seemingly routine. Agents arrive at dawn with arrest warrants and threats of long prison terms; they seize computers, storage devices,

ISSN 2049-1115 (Online). DOI: http://dx.doi.org/10.14318/hau5.2.022

and associated hardware (Coleman 2014: 135–36, 199). They turn prominent hacktivists into confidential informants and disrupt Anonymous networks with DDoS (Distributed Denial of Service) attacks (2014: 287, 303, 364).

However, despite its prominence as target and threat, the state remains an elusive presence at the edge of the community's perception. It breeds speculation and alarm (Coleman 2014: 296) but only manifests itself through its heavy-handed application of force. In this short comment we draw on HHWS's dazzling ethnographic content to begin mapping some of the emergent cyber strategies, tactics, and capacities the state deploys to complement its offline monopoly of violence. We sketch a repertoire of enforcement practices that have developed in part through the investigation and prosecution of the very hackers that populate Coleman's book.

Edgeworks of the state

In network theory, nodes are points where two or more lines transect. Nodes are centrally important in networks although the lines that link to only one node are considered peripheral. These lines are called edges and they are marginal because a network's strength is judged by the density of its nodes. Edges, existing on the outskirts of networks, can be seen as a computer-derived metaphor for fieldwork investigations of all types. Edgework is a concept in cultural criminology that emphasizes the phenomenology of transgressing boundaries (Lyng 1990, 2005; Garrett 2010). Adventure sports, dangerous fieldwork, undercover research, flirtations with illegality, et cetera (risk taking of all color) are examples of edgework.

HHWS is a master class in edgework: Coleman's account is riveting not just because it details how she infiltrated Anonymous and gained the trust of its more notorious participants but also because of the fine, precarious line she walks as ethnographer. For example, although she makes clear that any information she receives can't be given a guarantee of confidentiality (2014: 338) and her informants generally avoid providing her with sensitive intelligence, the mixture of excitement and alarm she documents among Anon communities in the summer of 2011 is palpable. As AntiSec hacks against law enforcement escalate and arrests become a common occurrence, Coleman reports weekly nightmares of "G-men" pounding on her door (300–302). Thus amid the narrative Coleman weaves we also gain a valuable insight into how power reconfigures in the pursuit of hackers and the particular edgework strategies of state actors themselves.

A case in point is Jeremy Hammond who Coleman first meets in IRC chats and later interviews in a Federal penitentiary where he is serving a ten-year sentence for hacking US military intelligence subcontractor Stratfor. Coleman offers a real-time depiction of the Stratfor operation from planning to the leak of 50,000 credit card numbers and five million emails to Wikileaks. In an IRC chat, Hammond tells Coleman, "about to rm-fm a major target" (in Linux vernacular—Hammond was going to erase the hard drive). The "major target" she finds out minutes later in a tweet from LulzSec member Sabu: "http://www.stratfor.com—#antisec dismantles a multi-million dollar intelligence corporation—watch the video and read the essay. #antisec." Coleman replies: "[H]oly sweet birth of the baby

Jesus, this is really happening!" (2014: 342). Readers are along for the ride, testing the edge of fieldwork, political dissent, and hacktivism.

It turns out that some of the sensitive information not disclosed to Coleman involved the possibility that Sabu was a government informant (2014: 339) and indeed Hammond, like many of the individuals in HHWS, is eventually caught. It came to light that Sabu *was* an FBI informant. Hammond's court documents were eventually leaked to journalists who claimed the FBI allowed Sabu to repeatedly break the Computer Fraud and Abuse Act to frame him (Coleman 2014: 358). Hammond testified to using a powerful zero day exploit that allowed him administrative access to a popular webhosting platform but it was Sabu and his FBI handlers that supplied him with the targets. It is here that Coleman's edgework, in turn, exposes the legal edges of the FBI's own investigation.

Hammond fed the acquired information—most of which was from foreign governments such as Turkey, Brazil, and Syria—back to Sabu and the FBI's servers (Coleman 2014: 358–59). What the FBI did with the assortment of stolen email accounts, databases, passwords, and backdoors it received is unknown—in part because Hammond's guilty plea ensures that much of the relevant information (internal emails and communication concerning the targets) will never be disclosed. Whether the FBI sought to map existing foreign vulnerabilities and exploits, perform intelligence gathering work on its (or another agency's) behalf, or whether this is a dysfunctional effect of the informant system where criminal investigators are allowed to routinely break the law as long as they are team players remains open to speculation (360).

In appropriating, learning from, and putting to work the methods of those already on the outskirts of legality, the FBI (and other government agencies) pursues a form of edgework that parallels the protest tactics of hacktivists; it explores the extremities of this social graph (what is legible and legal) while widening its sphere of action through the strategic use of ambiguous cyberlaws and the cover afforded by the mantle of state secrecy.

Tactics and strategies

As Coleman argues in relation to #operationpayback (2014: 127), de Certeau's "tactics" are a good way of describing the work of hacktivists. Though they infiltrate and breach state and corporate cyber infrastructures, their targets are shaped by opportunity and timing; they "make do" with whatever files or data they cull from breached servers and are flexible in the specific forms of resistance (zombie and voluntary botnets, propaganda, doxing, etc.) they employ. On the other hand though, despite ongoing state initiatives to surveil, monitor, regulate, and control the "space" of the Internet, it is not a terrain dominated by the state.

State strategy involves reading and mapping the quickly shifting terrain of online interaction until openings appear in the hacktivist community that bring particular targets within its line of sight. It is here that the state can bring to bear its particular strategic advantage (de Certeau 1984) by bringing proceedings under the mantle of its offline home terrain: the area of physical surveillance, arrests, searches, seizures, and incarceration. But until investigators are able to move proceedings offline, the

state must approach the "space" of the Internet much in the same way as hackers approach the terrain of the state. It must be nimble, flexible, and mobile: in short, it must use tactics.

For example, although IRC chat logs have now become a mainstay of courtroom proceedings and arrest warrants in hacktivist cases, investigators are sometimes wary of engaging in "undercover" work within chat rooms themselves. As one informant told us, joining a channel involves the certainty of being challenged by the room's participants and has the potential of corrupting an investigation (if criminal acts are coordinated or committed in the process) or disclosing its existence (or both). In lieu of undercover work and state proficiency in "passing" as members of the hacktivist community, state investigators focus on piercing the different "versions" of hacker identity to uncover the digital trails that link online personas with offline identities. The aim is to leverage hacktivists into becoming confidential informants (or zombie hackers) that will do the undercover work for the state.

In contrast, when online investigations seemingly take a more conventional form (such as the buying and selling of drugs), criminal investigators engage in a significant amount of covert work, swarming their targets with multiple lines of attack. For example, DHS agent Jared Der-Yeghiayan testified at convicted proprietor Ross Ulbricht's trial that during his investigation of the darknet drugs market Silk Road he had control over some eighteen user accounts. In addition to the six accounts he created on the forums and the market, Der-Yeghiayan assumed control of twelve accounts that he accessed through the consent or arrest of previous owners. Der-Yeghiayan took over the account of a low-level administrator on the site and worked his way up the administrator ranks into Ulbricht's inner circle. Alongside Der-Yeghiayan's Chicago branch of Homeland Security Investigations (HSI), another HSI agent based in Baltimore (Carl Force, now under criminal indictment himself) had been undercover for over a year, befriending Ulbricht and becoming his offline "muscle" and enforcer. Finally, the various HSI branches investigating Silk Road were not the only state agencies tasked with the Silk Road: the FBI, multiple US District Attorney's offices, the DEA, the IRS, the NSA, and other foreign law enforcement agencies were pursuing parallel and separate investigations.

The above "swarming" of agencies and the increasingly decentralized, nodal structure investigative forms take represents an inversion of the traditional silo approach to law enforcement where individual agencies had clear jurisdictional priority over certain categories of crime and clear distinctions existed between matters of internal and external security (Bigo 2000). As Richard Ericson notes in discussing the securitization of the state and the blurring of categories and control structures, "the view is that borderless threats require borderless law enforcement across organizational entities nationally and internationally, and across categories of citizens and non-citizens" (2007: 54–55). The Internet's claimed deterritorialization and decentralization has given rise not only to Anonymous, which has been described variously as a swarm, multitude, public, cloud, and a network, but also to a nimble, "disruptive," and entrepreneurial criminal investigative body.

Selfie-incrimination

Many scholars pathologize the taking of selfies as narcissistic (Keen 2015). For others, the selfie is a form of empowering self-representation (Nemer and Freeman 2015). Whatever the motives and interpretations, national security experts and law enforcement personnel see in social media a wealth of criminal evidence (Risen and Poitras 2014). The NSA agrees. The PRISM program ostensibly designed to preemptively catch criminals and terrorists, provides the NSA with backdoor access to the personal information stored by Google, Apple, Yahoo, Facebook, and other social media companies (Greenwald and MacAskill 2013). A 2012 poll of US law enforcement agents found that 80 percent searched online for information about suspects (Zadrozny 2015). Is it even possible not to self(ie)-incriminate?

Hacktivists have inadvertently provided self-incriminating evidence on social media in the form of selfies. In April 2012, Higinio O. Ochoa III, a member of Anonymous and LulzSec associated Cabincr3w, was charged by the FBI for hacking and releasing Arizona police officers' addresses and phone numbers. Ochoa posted a tweet linking to these documents under the name @Anonw0rmer. Associated with the tweet was an image of Ochoa's girlfriend's breasts above a sign bragging, "PwNd by w0rmer & CabinCr3w <3 u BiTch's !" The iPhone picture contained geolocatable metadata leading to further evidence and an arrest (Diaz 2012). Even when not being this unscrupulous, hacktivists have a difficult time not voluntarily leaving a digital trail.

In June 2015, Ross Ulbricht was sentenced to life in prison. Much like Ochoa, social media played an integral role in revealing his identity. He bragged on LinkedIn about "creating an economic simulation" outside the state and he asked on Google+ about parcel delivery services for the shipment of Silk Road purchased goods. He also posted a question and code (used within the Silk Road site) on the coder site, Stack Overflow, using his real name. The user agreements for both Google+ and LinkedIn assisted investigators in correlating Ulbricht and Dread Pirate Roberts but it was FBI investigator Chris Tarbell's coding knowledge that helped him connect Ulbricht's Stack Overflow question to the underlying code architecture of the Silk Road.

Even after the arrest of LulzSec (a group whose members were identified precisely because they shared personal details) and the centrality of good OpSec (operational security) to hacktivist operations, self-revealed evidence continues to substantially assist in the unmasking and prosecution of these groups. Is anonymity even possible in the current era of "infoglut" (Andrejevic 2013) where self and society compel our ceaseless self-projection and promotion online?

In the past, states went to extensive lengths to make their populations legible and readable; state interventions in society required the creation of "visible" units to observe, identify, monitor, and manipulate (Scott 1998: 183–84). Contemporary social media, in contrast, routinely generate nonstate platforms where individuals make themselves intimately legible in ways that advance and extend the state project of surveillance and social control. What is crucial here is not just that social media per se are premised upon visibility but that the legibility of individuals is a basic embedded component of online interaction and socialization.

Thus, what we describe as "selfie-incrimination" is not an exceptional "slip-up" but rather a persistent theme in the investigation and prosecution of hackers. It poses some novel questions about how mediated social forms are rewriting the public/private distinction, the state's role in pushing the boundaries of what "private" information can be pursued by public authorities, and the place that remains for democratic activism and political dissent in this reconfigured cyber-terrain.

Conclusion

Hacktivists and criminal investigators meet in zones of friction mediated by technology and law. This zone of friction is generated in a complex dialectic of "co-production" (Jasanoff 2004) and characterized by the "quintessentially local, messy, and contingent" character of the collective knowledge produced (Wolgar 2000: 168). Our short analysis illustrates the dominant position of the state: while knowledge about the other is coproduced, the state has resources with which to exploit this knowledge in ways hacktivists do not. Our goal has been to emphasize the entanglements of hacktivists and criminal investigators in acts of asymmetrical power coproduction; a dialectic that is generative of new practices, forms of knowledge, and applications of power the outcome of which remains undetermined. HHWS exhibits the mutually constitutive, antagonistic, and ultimately unequal coproduction in the field of hacktivist prosecution.

Further, if these new arrangements of power seem to favor the state they also complicate the way state strategies of control have conventionally countered the tactics of resistance. If part of the state's monopoly of force draws upon its strategic dominance over "place" and the capacity to render places visible and legible (de Certeau 1984: 36), the "placeless(ness)" of the Internet represents an adaptive challenge. Tactics become increasingly important not just as an "art of the weak" but also as an art of the state.

As de Certeau and HHWS remind us, the tactic is an artifact of contingency and placelessness. It takes shape on a terrain it does not own and "takes advantage of 'opportunities' and . . . must vigilantly make use of the cracks that particular conjunctions open in the surveillance of proprietary powers" (de Certeau 1984: 37). HHWS maps the cracks created by hacktivists and followed by criminal investigations. In the process, the state learns and adapts. Future ethnographies of the networked state and its strategies of prosecution and incarceration will need to follow in the steps of Coleman's exceptional fieldwork and explore the edges of legality toward this centralizing power.

References

Andrejevic, Mark. 2013. *Infoglut: How too much information is changing the way we think and know*. New York: Routledge.

Bigo, Didier. 2000. "When two become one: Internal and external securitisations in Europe." In *International relations theory and the politics of European integration: Power, security, and community*, edited by Morten Kelstrup and Michael Williams, 171–204. London: Routledge.

Coleman, Gabriella. 2012. *Coding freedom: The ethics and aesthetics of hacking.* Princeton, NJ: Princeton University Press.

———. 2014. *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. London and New York: Verso.

Coleman, Gabriella, and Alex Golub. 2008. "Hacker practice: Moral genres and the cultural articulation of liberalism." *Anthropological Theory* 8 (3): 255–77.

de Certeau, Michel. 1984. *The practice of everyday life*. Berkeley: University of California Press.

Diaz, Jesus. 2012. "These breasts nailed a hacker for the FBI." *Gizmodo*. http://gizmodo.com/5901430/these-breasts-nailed-anonymous-hacker-in-fbi-case.

Ericson, Richard. 2007. *Crime in an insecure world*. Cambridge and Malden, MA: Polity Press.

Garrett, Bradley. 2010. "Edgework." *Place Hacking*. http://www.placehacking.co.uk/2010/10/23/edgework/.

Greenwald, Glen, and Ewen MacAskill. 2013. "NSA Prism program taps in to user data of Apple, Google, and others." *The Guardian*. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Jasanoff, Sheila. 2004. *States of knowledge: The co-production of science and the social order*. London and New York: Routledge.

Keen, Andrew. 2015. *The Internet is not the answer*. New York: Atlantic Monthly Press.

Lyng, Stephen. 1990. "Edgework: A social psychological analysis of voluntary risk taking." *American Journal of Sociology* 95 (4): 851–56.

———. 2005. "Edgework and the risk-taking experience." In *Edgework: The sociology of risk-taking*, edited by Stephen Lyng, 3–16. New York: Routledge.

Nemer, David, and Guo Freeman. 2015. "Empowering the marginalized: Rethinking selfies in the slums of Brazil." *International Journal of Communication* 9: 1832–47.

Risen, James, and Laura Poitras. 2014. "NSA Collecting Millions of Faces from Web Images." *New York Times*. http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html.

Scott, James C. 1998. *Seeing like a state: How certain schemes to improve the human condition have failed*. New Haven, CT: Yale University Press.

Thacker, Eugene. 2004. "Networks, swarms, multitudes." *CTheory.net*, http://www.ctheory.net/articles.aspx?id=422.

Wolgar, Steve. 2000. "Social basis of interactive social science." *Science and Public Policy* 27 (3): 165–73.

Zadrozny, Brandy. 2015. "Crime-scene selfies: Generally a bad idea." *Daily Beast*. http://www.thedailybeast.com/articles/2015/02/09/crime-scene-selfies-generally-a-bad-idea.html.

Adam Fish
Department of Sociology
Lancaster University
Bowland North
Lancaster, LA1 4YN UK
a.fish2@lancaster.ac.uk

Luca Follis
Law School
Lancaster University
Bowland North
Lancaster, LA1 4YN UK
l.follis@lancaster.ac.uk