International Journal of Communication 10(2016), 1–20 1932–8036/20160005

Gagged and Doxed: Hacktivism's Self-Incrimination Complex

ADAM FISH[1]
LUCA FOLLIS
Lancaster University, UK

The investigation, arrest, and conviction of a number of high-profile hacker-activists, or hacktivists, reveal the ways subjectivity is mobilized through processes of revelation and evasion. We use the term *subjectivation* to describe the performative practices engaged in by hacktivists and contrast them with governmental and disciplinary practices of *subjection*. We elaborate upon two categories of subjectivation (*coming out* and *versioning*) and two categories of subjection (*doxing* and *gagging*). These categories form the vectors of hacktivist and state coproduction that emerge in selfie-incrimination. We use the term *selfie* to describe both intentional and inadvertent practices of online self-disclosure. Selfie-incrimination that is public and voluntary we discuss in terms of *coming out*. *Versioning* describes the public voluntary manipulation of personal identity. Being *doxed* entails the online disclosure of a hacktivist's identity. *Gagging* refers to this ultimate silencing of illicit political digital activity, wherein the state designates the parameters of speech as well as physical movement. We conclude by examining the entangled and asymmetrical relationship between hacktivist subjectivity and the cybersecurity of the state.

Keywords: crime, cybersecurity, hacker, hacktivist, identity, prosecution, selfie, state, stigma, subjectivity

Subjectivation and Hacktivism

Hackers are a distinct community who enjoy tinkering with computers and software, such as the German-based hacker organization Chaos Computer Club (Kubitschko, 2015) and the global open source movement (Kelty, 2008). These groups form a community around the sharing of best practices, knowledge, and software. The term *hacking* describes a varied set of practices involving a range of legal and also illegal acts. Hacktivists are individuals who use computers and networks to achieve political objectives. Ludlow (2013, p. 4) emphasizes advanced technological proficiency and political agency when

Adam Fish: a.fish2@lancaster.ac.uk
Luca Follis: l.follis@lancaster.ac.uk
Date submitted: 2016–04–29

[1] We would like to thank Majid Yar for reading and commenting on previous drafts, as well as the two anonymous reviewers for their stimulating comments. We would also like to thank Lauri Love for his continued inspiration.

he defines hacktivists as actors who use "technology hacking to effect social change." Their efforts include Internet Relay Chat discussions, distributed denial of service attacks, the production of propaganda videos, and the proliferation or *mirroring* of censored content (Fish, 2016). In this article, we focus on hacktivists who exfiltrate and publish information concerning the illegal or unethical activities of private companies or governments, which are sometimes called *cracking* (Jordan & Taylor, 2004, pp. 4, 17) or enforced transparency.

We describe the investigation, arrest, and conviction of a number of high-profile hacktivists. We focus on the powerful evidentiary role given to social media–derived personal data in these cases and analyze some of the adaptations and negotiations this engenders in hacktivist praxis. Today on social media sites, whether as a criminal, an activist, or an innocuous citizen—and regardless of whether they use encryption and pseudonyms—many people produce and leave a digital trail connecting to identities, preferences, political affiliations, and physical locations. If they are engaged in illegal activity, this evidence can be used against them in a court of law.

In light of the ubiquity of online personal data and its evidentiary power, we examine the chain of action that begins with the information management of hacktivist identity, its performative and practice-oriented disclosure, its eventual unmasking by investigators or rivals, and finally, the hactivist's bodily capture and internment by state actors. Our focus is on the self-directed and self-forming versions of subjectivity engendered by social media platforms. We adopt the term *subjectivation* to describe these performative practices engaged in by hacktivists and contrast them with governmental and disciplinary practices of subjection (Althusser, 1971; Butler, 2002; Foucault, 2002; Kelly, 2009).

Our understanding of subjectivation draws on Goffman's (1959, 1963) work on the performativity of public life and the patterns of concealment and disclosure linked to the management of a discredited or discreditable identity, as well as Foucault's (2002) emphasis on the active, agent-directed constitution of the subject. In contrast, we use subjection (Althusser, 1971) to refer to the broader process of subordination and subject creation that emerges in relation to dominating institutions of power. Subjectivation is central to the notion of performative politics and the sort of ethical skepticism of established power and knowledge relations Foucault associated with an Enlightenment critique (Butler, 2002, pp. 217–218; Foucault, 2002). In this context, subjectivation signifies practices of self-transformation that emerge in response to the obligations imposed by governments and their demands for unquestioning obedience. We understand hacktivism in similar politico-ethical terms, as a critical interrogation of state discourses of truth, the mechanisms of power they are bundled with, and the technologies of subordination they further. As a direct challenge to the technologies of the self pursued through governmentality and discipline, hacktivism can be understood as an "art of not being governed" (Foucault, 2002, p. 192).[2]

[2] Much has been made about how social media requires self-presentation (Goffman, 1959) and how modernity enhances the self-reflexivity (Giddens, 1991), or fluidity (Bauman, 2000), of daily life. Previous scholars have analyzed social media in terms first advanced by these scholars. For instance, Goffman's work has been used in the study of online "impression management" (Picone, 2015); Giddens's ideas have been used to connect reflexivity to digital democracy (Nothhaft, 2016); and Foucault's notion of discipline

Social roles—whether raced, classed, or gendered—are performed through routinized and public actions. Reflexivity is a central component of performative theory because it shapes how individuals learn to adopt different social positions. In contrast, hacker cultures, and digital cultures more generally, espouse a distinctive view of identity. Instead of a static and fixed persona, online culture encourages a performative skepticism (Butler, 1997) about the links between the online and off-line self. In the digital world, much like in postmodern linguistics, the signifier—one's profile picture, for instance—does not always correlate with what is signified—oneself (Derrida, 1978), and the differences between what is real and what is virtual can be exaggerated, understated, or subverted. Indeed it is precisely this hyperreality (Baudrillard, 1994) that forms the context within which the spectrum from transparency to anonymity exists.

In this sense, hacker identity is pliable, performative, and fluid, but this flexibility is premised on the ability to be, and remain, anonymous. These online performances are uncoupled from the "dramatic" and staged setting that usually comes with an off-line "audience" (Goffman, 1959, pp. 30–34), providing a space within which hacktivists can be whoever they claim to be. Yet the discrepancy, or gap, between these shifting "virtual" identities and the "actual" off-line social identity an individual possesses (i.e., the collection of attributes, characteristics, and signifiers that make the individual a socially distinguishable person) inevitably generates tension. It invites the deployment of information management techniques and patterns of revelation and concealment to manage the potential stigma of discovery and the "spoiling" of social identity (Goffman, 1963, pp. 12, 57, 164).[3]

Despite this tension, within the liminality of online performances, the literal technologies of selfhood—online platforms that afford virtuality, pseudonyms, and multiple identities—create the conditions for a pluralized and agential subjectivation. For example, the sort of "identity subsumation" (Sauter, 2014, p. 81) involved in joining Anonymous actions entails the temporary coming together of numerous, individual personalities under the mantle of the Anonymous meta-identity, a performance that is supported and reinforced by, among other things, the adoption of shared pseudonyms and "improper names" used by multiple participants (Deseriis, 2012). These practices multiply the reach of an

---

and Baumann's idea of liquidity have been used to critique online surveillance (Baumann & Lyon, 2013; Fuchs, 2013).

[3] A point of clarification is necessary here. In drawing on Goffman's work *Stigma* (1963), we have felt it necessary to update some of his categories for the digital age. The distinction between "virtual" and "actual" social identity is an obvious example. In Goffman's terms, "virtual" referred to the sort of impressions people draw about a person that they know little about. He contrasted this with "actual" social identity, which involved the sort of attributes and characteristics that an individual could be proved to possess and embody. In Goffman's analysis, then, the implication is that the latter is more "real," or more authentic, than the former. We do not make any claims of this sort; indeed, we follow the general direction of online scholarship, which argues that online, or "virtual," identities can be, in some respects, more real or authentic than their off-line counterparts precisely because in becoming free of those attributes, characteristics, and markers that define a person as "that kind of person," individuals are free to explore and develop identity in ways that more closely correspond to their inner preferences.

individual's actions and expand his or her performative repertoire while also blurring the lines between the swarming crowd and the individual (Sauter, 2014, p. 82).

Hacktivists engage in antagonistic, political, and often illegal work. As an "art of voluntary insubordination" (Foucault, 2002, p. 194), hacktivism targets power and questions its discourses of truth. This insubordination also inflects the form, content, and public perception of hacktivist dissent. Activists eschew the conventional normative and moral expectations publics have come to associate with traditional forms of protest or civil disobedience (e.g., the civil rights movement). Instead, groups like Anonymous cultivate an "outlaw persona" (Sauter, 2014, pp. 92–93), through which the valid political content of their message is rendered morally and politically "impure" (Shelby, 2015) by the unconventional form (e.g., profane, illegal, violent, offensive, pornographic, etc.) it takes. This not only invalidates the legitimate political character of the action but it also reinforces the association between this mode of activism and criminality. In short, hacktivist subjectivation does not happen in a vacuum and is not theirs alone to construct; rather, it emerges in a set of dialectical and coproduced interactions involving online communities, off-line publics, governmental institutions, and law enforcement authorities. For the latter groups, hackers represent a significant threat to the social order: They disrupt the long association between disciplinary technologies, punishment, and subjectivity (Thomas, 2003, pp. 180–181).

Hacking is made possible by the separation of body and identity in a virtual setting. For example, when one hacks into another's account or uses a stolen password, one is effectively performing that person's identity through the use of secret (or personal) authentication designed to confirm the current user is the genuine article (Thomas, 2003, p. 187). The investigation, prosecution, and conviction of hackers work to reconnect these virtual personas to the bodies and corresponding off-line social identities that theoretically own them. In this sense, the hacker's pursuit by law enforcement authorities becomes an occasion for the "reconstitution" of both hacker and subject (Thomas, 2003, pp. 185–186).

In seeking to hold hackers accountable, the state and its various apparatuses of hard and soft power condense these multiple "virtual" identities into one imprintable and imprisonable person (Butler, 1997, 2002; Foucault, 2002; Kelly, 2009). Indeed when rival hackers or law enforcement dox hacktivists or when they "come out" on their own volition, authorities begin a process of singularization designed to reinscribe the unmasked persona within state-derived categories and markers of social identity.

Thus, on the one hand, the goal of a criminal investigation is practical: It seeks to reconnect virtual identities with their embodied counterparts so that suspects can be named in investigative and court documents, can be physically located and surveilled, and can ultimately be held behind prison walls, in digital exile. On the other hand, however, this reconstruction of "actual" social identity is a process that sets the stage for the conversion of a discreditable person (one who obfuscates or systematically frustrates the disjuncture between virtual and actual off-line identity) into a discredited person (Goffman, 1963). It furthers media narratives and public anxieties concerning the current intersection of technology and identity as well as the dangers posed by anonymity and the dark recesses of the Web. State practices of stigmatization and degradation—as well as the application of labels like *criminal, terrorist*, or *felon* to hacktivists (Goffman, 1963)—feed into these anxieties and supplement these narratives. Ultimately, these are as much transformational practices (Garfinkel, 1956) aimed at the subjugation of the self as they are

exercises of symbolic power directed at the public (Bourdieu, 1994). We adopt the term *subjection* (Althusser, 1971, pp. 133–181) to describe these official efforts in singularization and stabilization.

In the sections that follow, we describe the investigation, arrest, and conviction of a number of high profile hacker-activists, or hacktivists. We elaborate on two categories of subjectivation (*coming out* and *versioning*) and two categories of subjection (*doxing* and *gagging*). These categories form the vectors of hacktivist and state coproduction that emerge in selfie-incrimination (see Figure 1). We use the term *selfie* to describe both intentional and inadvertent practices of online self-disclosure. We discuss selfie-incrimination that is public and voluntary in terms of coming out. Versioning describes the public voluntary manipulation of private identity. Being doxed entails the online disclosure of a hacktivist's real-world identity. Gagging refers to this ultimate silencing of illicit political digital activity, wherein the state designates the very parameters of speech as well as physical movement. We conclude by examining the entangled and asymmetrical relationship between hacktivists and the state.[4]

	Public	Private
Involuntary (Subjection)	Outed; doxed	Gagging; imprisonment
Voluntary (Subjectivation)	Coming out; whistleblower	Anonymity; versioning (public voluntary manipulation of private identity)

Figure 1. The Selfie-Incrimination Complex.[5]

Selfie-Incrimination and Versioning

We use the term *selfie* in a manner distinct from the way in which it is commonly used. While some analysts pathologize this mode of self-expressivity as narcissistic (Keen, 2015) and others understand it as a form of empowerment (Nemer & Freeman, 2014), we use it as an umbrella term that designates all the artifacts that result from the convergence of social media, online performances, and criminal prosecutions. We therefore perceive this axiomatic and ubiquitous mode of contemporary self-

[4] In collecting data for this project, we used a mixed methodology that combined the examination of primary documents and interviews with alleged hacktivists, lawyers, and criminal investigators. We sought to collect data about the techniques used by both hacktivists and criminal investigators. To this end, we read and examined all available court documents for Silk Road founder Ross Ulbricht, whistleblower Chelsea Manning, hacker Andrew Auernheimer, and Anonymous associates Barrett Brown, Jeremy Hammond, Matt DeHart, Lauri Love, and Hector Xavier Montsegur. We also examined primary documents produced by Edward Snowden and Julian Assange.

[5] While our analysis reinforces a public-private divide, we believe the boundary between them is less fixed than often assumed. Social media makes the boundaries separating the public and the private less stringent.

expression through the lens of law enforcement and national security experts, who see a wealth of criminal evidence in social media (Risen & Poitras, 2014). For example, a 2012 poll of U.S. law enforcement agents found that 80% searched online for information about suspects (Zadrozny, 2012, para. 13). *New York Times* investigative reporter Ian Urbina writes, "[S]ocial media has been a boon for law enforcement, handing the police ready admissions of guilt, equipping criminal investigators with new types of evidence and empowering prosecutors to better dispel reasonable doubt of guilt (2014, para. 1)..

Our argument is that much like others in the "self(ie) generation" (Blow, 2014)—socially liberal, digitally literate 18–33-year-olds—hacktivists are quintessential networked selves, whose identity is built up around online performances, playful uses of networks, and competencies with digitally derived vernaculars. The persistence, scalability, replicability, and searchability of social media make it difficult to erase personal information (boyd, 2010). Hacktivists use social media as a platform for the performance of their activist selves, and in the process often provide the very digital breadcrumbs that lead to criminal investigations. The present digital culture centered around the pervasive collection of volitional and amateur content by corporate and government bodies is personified in the concept of the selfie—a political as well as an economic system of self-surveillance.

Selfie describes both intentional and inadvertent practices of online self-disclosure. While self-representation with images, video, and social media has become a quintessential form of self-expression and identity performance, it poses a paradox for the hacktivist who uses computers, networks, email, and social media to acquire and disseminate political information. With every selfie comes a risk of self-incrimination, or *selfie-incrimination*. Higinio O. Ochoa, a member of Cabincr3w (which is associated with Anonymous and Lulzsec), who was charged with hacking and releasing Arizona police officers' addresses and phone numbers, is a case in point. In April 2012, Ochao posted a tweet linking to these police 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 !" (Diaz, 2012, p. 3). The iPhone picture contained geolocatable metadata that led to further evidence and his arrest. While few activists are brazen enough to post an actual selfie, hacktivists find it difficult to not selfie-incriminate.

In the context of this predicament, hacktivists and their pursuers use an assortment of "virtual" identities to obfuscate the links between their online and off-line identities (Brunton & Nissenbaum, 2015). In an effort to elude selfie-incrimination, they seed misinformation through the practice of versioning. In the software industry, versioning refers to the process by which a new iteration of software acquires a new categorical identity. For example, the read-write Web 2.0 is seen as an incremental improvement version over the read-only Web 1.0. Versioning signifies the "bootstrapping," or processual nature, of startup and software culture, wherein developers are encouraged to release software early and update it often. Like multiple identity performativity, another software version is not entirely new. Rather, it is the core product with different features. We introduce the concept of versioning as a way to describe the unstable, flexible, and performative character of hacktivist identities online.

Anonymity, pseudoanonymity, privacy, and secrecy (while not guaranteed by even the most robust cryptography) are pursued in online spaces that do not have "real name" policies such as Facebook. Within these spaces a single hacker might adopt numerous screen names—in short, different

versions of him- or herself connected with immediate practical tasks. For example, the hacktivist Jeremy Hammond went by a series of aliases—"Anarchaos," "sup_g," "burn," "yohoho," "POW," "tylerknowsthis," "crediblethreat," "ghost," "anarhacker," "O"—on Internet Relay Chat (IRC) channels while discussing ongoing hacks and planning new operations (U.S. Attorney's Office for the Southern District of New York, 2012). This also means that versioning requires significant interpretive work: Hactivist discussions take place among individuals who may have never met face-to-face, guard their off-line personas, and deploy multiple versions of themselves contemporaneously. Interlocutors must be capable of tracing the continuities between these different hacktivist iterations so that they can have a reasonable sense of "who" they are talking to or, at the very least, whether they are law enforcement.

The pliability and flexibility of the networked self means that law enforcement can also practice versioning. During his investigation of the Silk Road market, Homeland Security Investigations (HSI) agent Jared Der-Yeghiayan acquired access to some 18 user accounts (U.S. District Court for the Southern District of New York, 2015, pp. 693–694). In addition to the 6 accounts he created on the forums and on the market, Der-Yeghiayan commandeered 12 accounts through the coerced consent or arrest of previous owners. Early into the investigation, he took over the account "cirrus" from a low-level site administrator (U.S. District Court for the Southern District of New York, 2015, pp. 691–692). Posing as "cirrus," he became a trusted insider and worked his way up the ranks into the Silk Road's managerial circle (U.S. District Court for the Southern District of New York, 2015, p. 728).

Similarly, HSI agent Carl Force worked undercover for over a year, befriending convicted Silk Road "mastermind" Ross Ulbricht (aka Dread Pirate Roberts [DPR]) and becoming his off-line enforcer. In addition to his covert work, Force created a series of unauthorized, virtual personas to communicate with DPR. With one of these he attempted to extort $250,000 from Ulbricht in exchange for not providing incriminating information to law enforcement (U.S. District Court for the Northern District of California, 2015, p. 3). He also arranged a fake murder for DPR, under the moniker "Nob," and was paid $100,000 by Ulbricht as "French Maid." As "Death From Above" he told DPR that he was a Green Beret and friend of the man allegedly killed by "Nob," who was going to kill Ulbricht (Greenberg, 2015). Although seemingly empowered by the performativity of the networked self and its capacity for anonymity, Force—much like the hacktivists discussed previously—was the victim of his own selfie-incrimination (he was recently sentenced to 6.5 years for bitcoin money laundering and wire fraud associated with the Silk Road investigation).

Versioning lays bare the process-oriented, performative nature of hacktivist online identities. It targets the strategies of self-presentation, identity management, and "face work" (Goffman, 1959, 1967) that dominate actor performances in the off-line world. In contrast, social media platforms like Facebook and Google+ seek to extend these interaction structures: They use processes of replication, correlation, and indexing to chart an actor's off-line associations so that they can be directly ported into digital form. Though the end product is more scalable, nuanced, and actor directed, the effect is to reify and confirm a singular "actual" social identity that is already categorically fixed in the off-line world.

The manifold nature of identity performances challenge any static perspectives on subjectivation. Versioning is an exercise in agential self-creation that exploits the pseudo-anonymous affordances of

social media and provides a space for the performance of multiple, virtual selves. Versioning is also a practice performed by the state, whose identity deceptions embolden investigators in virtual worlds. Once there, a process of corralling and cross-referencing unfolds whereby the winnowing of pseudonyms, biographical fragments, and personal characteristics may eventually lead to the linking of online and off-line identities. In an unexpected about-face, aliases designed to evade self-incrimination become informants aiding in an individual's capture.

Coming Out

Some hacktivists willingly disclose their identities while in pursuit of information they find germane to the public interest. Whether they label their actions as investigative journalism or whistleblowing, the rationale for self-exposure flows from the motivation to bring to light the illicit, illegal, or unethical practices committed by governments or corporate institutions. At times, self-identification is an inevitable part of the process of information liberation since information about the data's provenance is necessary to legitimate and authenticate it, but at other times the decision to cross the threshold between off-line and online social identity is deliberate and calculated.

Understood in the context of the impression management and information control strategies (Goffman, 1963) deployed by actors to negotiate the "discrepancy between virtual and actual identities that when made known or apparent spoils his social identity and discredits him," voluntary disclosure can appear as a strategic moral and political turning point (Goffman, 1963, pp. 31, 125). Earlier we drew on the concept of "impure dissent" (Sauter, 2014; Shelby, 2015) to illustrate the point that hacktivist political communication is rendered morally and politically illegitimate because of the unconventional form it takes or the content with which it comes bundled. A central characteristic that helps render the motives of hacktivists morally and politically suspect (besides its illegal or controversial facets) is the use of anonymity. Indeed as Sauter (2014, pp. 90–92) has argued, Anonymous activism brings to the fore the extent to which assigning a politically responsible motive to dissent is predicated on the Western expectation that if critique and civil disobedience are to be labeled legitimate, they must be performed through a state-sanctioned and socially transparent identity. Coming out involves reclaiming political responsibility and legitimacy through self-disclosure and revelation. It is an attempt to shape social identity in the court of media or public opinion and outside the stigmatizing narratives of the state.

The mainstream media play an important role in manifesting hacktivists' goals of bringing attention to political causes. For some, coming out is a necessary component of gathering media attention. Take Julian Assange, for instance. Largely because of the way journalists have framed the story, it is now difficult to differentiate between Wikileaks and Assange's persona. A brief exchange in the documentary *We Steal Secrets* (2013) provides a glimpse into the paradoxes generated by the spotlight. While a Swedish makeup artist applies bronzer to his face, the videographer Mark Davis asks a question that illustrates the tension between Assange's publicity and the operation's secrecy: "WikiLeaks needs a face?" To which Assange responds,

> Yeah, well, the public demands that it has a face. And actually we'd much prefer—I'd prefer —that it didn't have a face. We tried to do that for a while and people just, the demands were so great people just started inventing faces. (*We Steal Secrets*, 2013)

Assange describes his notoriety as a kind of martyrdom—"It is my role to be the lightening rod to attract the attacks against the organization for our work" (*We Steal Secrets*, 2013)—and it is clear that this increased visibility has been double-edged. He is wanted for extradition by Swedish authorities and remains under siege at the Ecuadorian embassy in London, where he has sought refuge for over three years. On the other hand, by giving the organization a prominent mouthpiece and spokesperson, Assange is able to articulate a coherent ethical frame to recast the work of Wikileaks as an act of political dissidence, protest, and critique.

Like Assange, Edward Snowden, the whistleblower of the NSA's secret, unwarranted, and bulk surveillance programs, decided to come out. In May 2013, Laura Poitras filmed Snowden watching world events from a room in Hong Kong's Mira Hotel as the *Washington Post* and *Guardian* began reporting on the leaked material. Poitras assumed that he would want to remain anonymous but Snowden had long planned to out himself: "I will be identified, and my footprint will be left once the documents are published, and the government will know" (Ehrlich, 2014, p. 5); he also knew that his footprint would guard against anyone questioning the authenticity of the material (O'Hehir, 2014).

He eventually agreed to being filmed and told Poitras, "I hope you will paint a target on my back and tell the world I did this on my own" (Harding, 2014, p. 37). The target painted by Poitras (a short video released by the *Guardian*) shows a reflexive young man motivated by a sense of public duty: He blew the whistle to prompt a sustained public debate about the otherwise private and illegal actions conducted by the United States and its allies. In contrast to the celebrity and scandal swirling around Assange, Snowden's eloquent recasting of his actions under the banner of democratic constitutionalism seemingly increased his credibility and the significance of his actions.

The Justice Department response was predictably swift and severe: Snowden is wanted for extradition and has been charged under the 1917 Espionage Act for communicating national-defense information without authorization and for revealing classified information (Finn & Horwitz, 2013). President Obama's adviser on Homeland Security and Counterterrorism, Lisa Monaco, invited Snowden to "come home to the United States, and be judged by a jury of his peers" (White House, 2015, p. 5). Like all whistleblowing, coming out involves accepting the consequences of one's decision. Indeed Snowden has repeatedly sought a plea deal involving jail time from U.S. authorities as long as he is not cast as "a deterrent to people trying to do the right thing in difficult situations" (Graham, 2015, p. 2).

Assange and Snowden illustrate the extent to which subjectivation and subjection are co-created—as well as the competing discourses of truth unleashed by whistleblowing. Hacktivists claim that their actions have a critical purpose and an ethical motivation. At the same time, the state simultaneously claims that their actions reveal who they really are (i.e., criminals, terrorists, spies) and the danger they pose to the body politic.

Another individual who came out is Barrett Brown, a freelance journalist who had written for *Vanity Fair, The Huffington Post, Business Week,* and *The Guardian*. He had been affiliated with Anonymous for a number of years and first logged into the AnonOps server using his real name when Operation Tunisia (in support of pro-democratic activists) began—in the process, violating the core precepts of anonymity and radical equality that animated the community. Discussing this moment in an IRC chat a short time later, Brown wrote: "I have been Anon for five, six years, came out two months ago. I have got a plan" (U.S. District Court for the Northern District of Texas, 2014, p. 46). In the period that followed, Brown invited publicity, offering himself as a mouthpiece for Anonymous and speaking openly to reporters, penning press releases, and posting videos of himself online. Ironically, it was an interview he gave with *Russia Today* during an ongoing Anonymous operation (in retaliation for the takedown of the site MegaUpload by U.S. authorities) that first brought him to the attention of Federal Bureau of Investigation (FBI) agents (U.S. District Court for Northern District of Texas, 2014, p. 22).

Brown adopted a constantly shifting arsenal of descriptors that simultaneously linked him to the fourth estate ("journalist," "former journalist," "pseudo-journalist") and Anonymous ("propagandist," "informal spokesperson," "strategist," "theorist," "operative," "forward engineer," "legal organizer") a practice that recalls the mutable and performative construction of identity we term versioning, but that also illustrates a consistent strategic rationale. He used his public persona, journalistic credentials, and outsider status to carve a liminal space from which he could use the fruits of Anonymous hacks and operations for investigative purposes.

Though prosecutors originally charged Brown with 10 counts of aggravated identity theft and two counts of credit card fraud for posting an HTTP link to leaked emails from Stratfor, these charges were eventually dropped when he pleaded guilty to the crimes of accessory, obstruction, and threatening a federal officer in exchange for a deal (U.S. District Court for the Northern District of Texas, 2012). It is unclear how successful the prosecution's case could have been had Brown not threatened FBI Agent Robert Smith via a YouTube video, since he was always careful to point out that whatever his involvement with Anonymous, he did not hack. This is also illustrated by the fact that other journalists who had posted the same HTTP link were never charged and that throughout his trial Brown was under a gag order that prevented him from speaking to the media.

In coming out, hacktivists attempt to govern their subjectivation by controlling their name and the time of its publicity. For Assange, subjectivation meant Wikileaks grew to prominence. In Snowden's case it meant he could take responsibility for, and justify, his actions. Brown thought an identity as a journalist might give him constitutional cover. Each hoped to manage the public's understanding of the motivations surrounding their actions so that debates concerning the political import of their disclosures and revelations remained focused on the content of the communication—and not tainted by the renegade identity of the messengers. In this sense, coming out is an effort toward dignity and, however futile, toward retaining agency in the face of mounting subjection.

Doxing

The clearest example of the tensions posed by the networked and illicitly political self play out around the category of being discovered, revealed, outed, or doxed by criminal investigators, former collaborators, or police informants. Doxing refers to the exposure of personal and previously private information (e.g., home address, phone numbers, credit card numbers, pictures, financial records, etc.) about an individual online; it originates from "docs," itself short for "documents." Doxing is a popular hacktivist tactic deployed against a wide array of marks including law enforcement, corporate executives, and private security contractors. *Doxers* build dossiers about targets that are then released in various online locales (e.g., sites like Wikileaks, Pastebin, Doxbin on the Tor "dark net," social media networks, and online forums) in an effort to embarrass and harass individuals or their organizations.

Doxing has a leveling and flattening effect on power asymmetries: It targets and neutralizes the wall of privacy and anonymity that often characterizes the upper echelons of corporate industrial power and pierces the "faceless" and uniformed persona of its foot soldiers. For example, in response to a series of dawn law enforcement raids and covert activities against hacktivist groups Anonymous and LulzSec in 2011, FBI agents were warned via the Anonymous-related Twitter account @OpMonsanto to expect the release of their personally identifiable information: "To any FBI agent involved in the continued unjust raiding of peaceful Anons: Expect us. You are no longer entitled to your privacy" (Federal Bureau of Investigation, 2011, p. 4).

Anonymous followed up this missive a few days later by hacking more than 70 law enforcement websites and exfiltrating large amounts of confidential data, including email addresses, user names, social security numbers, home addresses, phone numbers, informant lists, active warrant information, and databases of jail inmates. This operation eventually involved the doxing of some 7,000 police personnel and led the FBI to issue an Intelligence Bulletin warning personnel to protect themselves against the high risk of identity theft and harassment caused by doxing (Federal Bureau of Investigation, 2011).

With the exception of self-outing, the default setting of hacktivist communities is anonymity, and it is rigorously pursued through operational security and versioning. Yet the notoriety of hacktivist operations, intrusions, and data dumps—as well as their increasingly political and destabilizing effect—has generated strong incentives for cyber-mercenaries, rival hackers, law enforcement personnel, and private security outfits to dox hacktivists.

One well-documented example involves the private security firm HBGary Federal and its attempts to dox key members of Anonymous, map the organizational hierarchies of the group, and present the findings at the Bsides security conference in 2011 under the title, "Who Needs the NSA When We Have Social Media?" In advance of the presentation, the company's CEO, Aaron Barr, claimed to have infiltrated Anonymous, discovering its command structure and the identities of its key members (Menn, 2011). The very day Menn's *Financial Times* article broke, Anonymous hacked into HBGary Federal and its parent company's websites, downloaded email spools, and deleted files and backups, as well as commandeering all of Barr's social media accounts. Most of the company emails and documents were eventually posted on

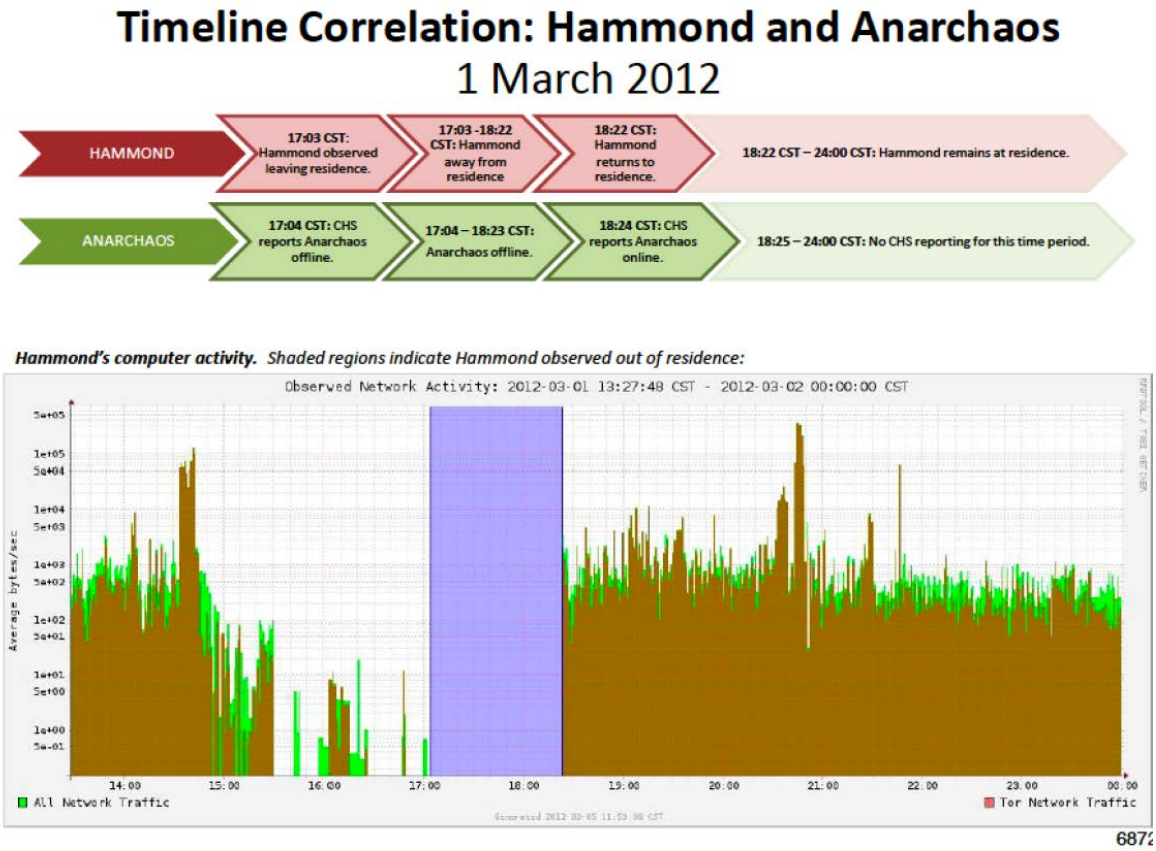
the Pirate Bay and AnonLeaks, leading to a series of scandals and, after Barr's resignation in February 2011, HBGary Federal closed its doors (Coleman, 2014).

Barr's overall methodology of cross-referencing and correlating user information on IRC, Facebook, and other sites to draw connections between users, their relationships, and their activity is precisely the sort of information the FBI used to identify the hacktivist Jeremy Hammond. Hammond's case illustrates the efficacy of these investigative online methodologies when combined with the off-line resources of federal law enforcement. Like many hacktivists, Hammond deployed a variety of online personas and nicknames in his exchanges on instant messaging, chat, and social media platforms. A central clue to Hammond's real-life identity was obtained first through the deconstruction of his versioning (e.g., determining that Hammond was, in fact, "sup_g," "yohoho," "ghost," etc.) and then the correlation of the biographical clues he had inadvertently provided through these different aliases.

An influential member of Anonymous, Hector Xavier Montsegur ("Sabu"), was arrested by the FBI in June 2011 and subsequently informed on Hammond. From June onward, Sabu incited, helped plan, and executed a variety of notorious hacks while working for government authorities. As is evident in the numerous IRC chats the government introduced as evidence against Hammond, Sabu would attempt to link Hammond's different online identities (Anderson, 2012). For example, in a chat log between Sabu and Hammond as "sup_g" where they discussed the fallout from the Stratfor hack, at a certain point Sabu stated, "If I get raided anarchaos your job is to cause havok in my honor." "Anarchaos" was one of Hammond's numerous identities, and Hammond's reply of "it shall be so" drew a connection between the two personas (U.S. Attorney's Office for the Southern District of New York, 2012, p. 22).

At the same time, Sabu's identity as the most militant and publicly outspoken member of Anon invited trust, so Hammond sometimes volunteered information. For example, in an IM conversation with Sabu in January 2012, Hammond, as "yohoho," asks Sabu (as "leondavis") to help him meet a member of the hacktivist outfit "cabincrew," Sabu directs him to the cabincrew IRC channel and Hammond asks him to "invite sup_g" so he can enter the channel; moments later he corrects himself and asks that Sabu invite yet another alias, "an0n4g" (U.S. District Court for the Southern District of New York, 2014, Exhibit H, p. 8). At other times, as other personas, Hammond disclosed that he had served time in federal prison, had been arrested and detained at the 2004 Republican National Convention, and had done some time for marijuana possession, among other personally identifying information (U.S. Attorney's Office for the Southern District of New York, 2012, pp. 26–29).

The FBI used Sabu's chat files (Sabu had been using a government issued laptop and was under 24-hour surveillance) to isolate the kernels of biography and online activity Hammond disclosed and compare them to law enforcement records. Once they were reliably sure that Hammond was their target, FBI agents began surveillance, physically staking out his house on the Southside of Chicago and using a "pen register" device to reveal the Internet Protocol (IP) addresses of the sites he was visiting. As Figure 2 illustrates, physical surveillance dovetailed with online surveillance as investigators used Sabu to check if Hammond's arrival or departure from home correlated with the appearance or exit of one of his online personas.



Source: Federal Bureau of Investigation, 2012

Figure 2. March 1, 2012: FBI Surveillance of Hammond's TOR Activity.

Although the motivation and ultimate manifestation of doxing practices varies, one can identify two broad patterns. For hacktivists, doxing is an end in itself: The public exposure of individuals, organizational hierarchies, and intimate connections is a highly symbolic, overt act. In many respects, it causes the now-ubiquitous practices of surveillance and visibility to be diffused among the general public against its operators—or at least their symbolic proxies. In contrast, as a countertactic deployed by law enforcement and private security contractors, doxing is covert and serves as a means to an end. That goal might involve the development of a dossier on an individual or a group of hacktivists to use as a starting point for deeper and more intrusive surveillance that will eventually form the basis for an arrest (e.g., Jeremy Hammond) or as a final component in the effort to turn hacktivists into confidential informants (e.g., Sabu).

Doxed individuals are often informed on by a former colleague or confidant who has been turned into an informant by authorities. Search-and-arrest warrants may soon follow, drawing together more evidence and cataloging the connections between the virtual and off-line worlds. Whatever agency remains to the hacktivist at this point will have to be asserted in a court of law under the threat of state subjection.

Gagging

A gagging order is a legal injunction that suppresses public speech; it has been previously used to silence hackers like Kevin Mitnick (Mitnick, 2012). It may be implemented so that private or sensitive information does not become public in the course of a prosecution. Additionally, imprisonment, though imposed to punish and reform criminals, can also have a silencing effect on political speech. Besides restrictions and limitations surrounding prisoner correspondence, visiting and phone privileges, the "totalizing" character of prison regimes is designed to atomize and isolate. There have been some notable cases of hacktivists that managed to send a few tweets from behind bars with the aid of friends on the outside (e.g., Barrett Brown). But for prisoners whose cases carry strong subversive and political implications or hacktivists who can become spokespersons and martyrs for political causes, routine security constraints on communication can become de facto injunctions against it.

Despite the scrupulous anonymity maintained by hacktivists, many are eventually unmasked, surveilled, and caught. They are often placed under court orders restricting what they can say in public and sentenced to lengthy prison sentences. Moreover, when they are released, they can only look forward to living a largely analog life. For example, in 2013, Jeremy Hammond was sentenced to a maximum of 10 years in custody and another three years of supervised release. Throughout the trial he was under a court order that restricted what he could say in public, and although the government's discovery materials involved three terabytes of documents, he was only able to view the material in the presence of his lawyers and could not use prison computers to do legal research—despite the fact that they are not connected to the Internet (Reitman, 2012). While in prison, he is allowed to use the nonprivate Federal Prison Email service (Trust Fund Limited Inmate Computer System [TRULINCS]) to keep in touch with authorized contacts.

Upon release, Hammond will be subjected to a series of special supervision conditions for three years. These include a prohibition on involvement or contact with electronic civil disobedience websites or organizations, participation in the probation department's computer/Internet-monitoring program, a complete ban on masking online identity, and a ban on the encryption of stored data and online communications (e.g., through TOR or proxy servers)—although these may be allowed if undertaken as part of legitimate employment (U.S. District Court for the Southern District of New York, 2014, p. 75). Further, Hammond's computer and connected devices will need to be registered with the probation department and outfitted with surveillance applications that will monitor his activities.

Similarly, throughout his trial, Barrett Brown was under a court-imposed gag order that prevented him from speaking with the media. He was sentenced to five years in prison and two years of supervised parole after he is released. The restrictions on Brown's supervised release mirror Hammond's:

He will have to enroll in the probation service's computer- and Internet-monitoring program, pay for the costs of his monitoring, and comply with the installation of hardware and software that allow for "the evaluation of [his] computer use" (U.S. District Court for the Northern District of Texas, 2014, p. 318). He will also be required to submit to periodic and unannounced examinations of his computers and associated hardware as well as provide written authorization for the release of information from his Internet service provider.

Prisons have always leveraged the contrast between inside and outside as a mechanism for institutional control (Irwin, 1985), but increasingly they also heighten and exaggerate the gap between the online and off-line. In this sense, a custodial sentence not only interrupts the acts of subjectivation and self-formation described in this article, it also forms the institutional harness through which dominant categories of individual ascription and identification are redeployed. In prison only one identity (conferred and guaranteed by the state) is recognized as valid and legitimate. Further, release from imprisonment under the special parole conditions described previously extends this targeted reinscription of identity into the community. Even though prohibitions and injunctions against the use of computers for convicted hackers have been meted out as conditions of release since the mid-1990s (e.g., for Chris Lamprecht, Kevin Mitnick, and Kevin Poulsen) (Thomas, 2003), these new, legally imposed bans on dissent, anonymity, and encryption associate digital activism and online civil disobedience with a presumption of criminal intent, thereby transforming subjectivation practices into technologies of subjugation. That is, they have been transformed into a set of techniques that reinforce and reify traditional mechanisms of state control premised on ensuring the legibility and visibility of subjects and their stigmatized classification.

Conclusion

An examination of the conviction of hacktivists reveals the performative practices of hacktivists (subjectivation) and the disciplinary practices of the state (subjection). Hacktivists and cyberlaw enforcement are in an uneasy relationship in which each co-creates the other. We have argued that this asymmetrical space of co-creation takes shape against the backdrop of a digital culture animated by amateur and voluntary practices of self-presentation (encapsulated by the term *selfie*) that have both emancipatory and constraining effects. In particular, we have highlighted the extent to which corporate systems of surveillance and state modes of subjugation are embedded and furthered through the practices of self-presentation and emancipation that are engendered by digital culture.

In this article, we focused on hacktivists who infiltrate government and corporate servers. In pursuing them, investigators further develop their arts of cracking and identity versioning. It is a dialectical process. New generations of hackers develop new techniques in evasion and infiltration, and in response, a new criminal division lurches forward to investigate. This process evolves into the future, with the state, for the most part, dominating the eventual direction of the relationship (Fish & Follis, 2015). As investigations into hacktivist "know-how" and state counterstrategies, these explorations of networks and computers are epistemological pursuits involving technology, computer science, jurisprudence, and the flexible identities afforded by social media platforms. They illustrate the ''quintessentially local, messy,

and contingent'' (Wolgar, 2000, p. 168) process of knowledge coproduction and its "awkward, unequal, unstable" (Tsing, 2005, p. 4) character.

As either activists for a more open society or unscrupulous users of technology, there is much to learn about identity and how the state evolves in response to the pursuit of hacktivists. We have focused on how identity is a multipurpose tool for both criminal investigators and hacktivists. Like whistleblowers, hacktivists are considered by some to be public servants, making corporations and politicians more transparent. Others see hacktivists as avant-garde techno-criminals, on the vanguard of cyber-insecurity. Whether one sees the practices of hacktivists as benevolent or illegal, one thing is certain: The future of illicit digital activism is being constructed through the relationship between hacktivists and the state.

References

Althusser, L. (1971). *Lenin and philosophy and other essays*. New York, NY: Monthly Review Press.

Anderson, N. (2012, March 7). Stakeout: How the FBI tracked and busted a Chicago anon. *Ars Technica*. Retrieved from http://arstechnica.com/tech-policy/2012/03/stakeout-how-the-fbi-tracked-and-busted-a-chicago-anon/

Baudrillard, J. (1994). *Simulacra and simulation*. Ann Arbor, MI: University of Michigan Press.

Bauman, Z. (2000). *Liquid modernity*. Cambridge, UK: Polity Press.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance.* London, UK: Polity Press.

Blow, C. (2014, March 3). Self(ie) generation. *The New York Times*. Retrieved from http://www.nytimes.com/2014/03/08/opinion/blow-the-self-ie-generation.html?_r=0

Bourdieu, P. (1994). Rethinking the state: Genesis and structure of the bureaucratic field. *Sociological Theory*, *12*, 1–18.

boyd, d. (2010). Social network sites as networked publics: Affordances, dynamics, and implications. In Z. Papacharissi (Ed.), *Networked self: Identity, community, and culture on social networking sites*. New York, NY: Routledge.

Brunton, F., & Nissenbaum, H. F. (2015). *Obfuscation: A user's guide for privacy and protest*. Cambridge, MA: MIT Press.

Butler, J. (1997). *The psychic life of power: Theories in subjection.* Stanford, CA: Stanford University Press.

Butler, J. (2002). What is critique? An essay on Foucault's virtue. In D. Ingram (Ed.), *The political* (pp. 212–229). Malden, MA: Blackwell Publishers.

Coleman, E. G. (2014). *Hacker, hoaxer, whistleblower, spy: The many faces of Anonymous*. London, UK: Verso.

Derrida, J. (1978). *Writing and difference*. Chicago, IL: University of Chicago Press.

Deseriis, M. (2012). Improper names: Collective pseudonyms and multiple-use names as minor processes of subjectivation. *Subjectivity*, *5*, 140–160.

Diaz, J. (2012, April 12). These breasts nailed a hacker for the FBI. *Gizmodo*. Retrieved from http://gizmodo.com/5901430/these-breasts-nailed-anonymous-hacker-in-fbi-case

Ehrlich, D. (2014, October 20). Laura Poitras on the exclusive Edward Snowden access that created *Citizen Four*. *The Dissolve*. Retrieved from https://thedissolve.com/features/interview/791-laura-poitras-on-the-exclusive-edward-snowden-acce/

Federal Bureau of Investigation. (2011, August 2). Law enforcement at risk for harassment and identity theft through "doxing." *Intelligence Bulletin, FBI Cyber Intelligence Section*. Retrieved from https://info.publicintelligence.net/FBI-Doxing.pdf

Federal Bureau of Investigation. (2012). Timeline correlation: Hammond and Anarchaos. Retrieved from http://www.documentcloud.org/documents/1342115-timeline-correlation-jeremy-hammond-and-anarchaos.html

Finn, P., & Horowitz, S. (2013, June 21). U.S. charges Snowden with espionage. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html

Fish, A. (2016). Mirroring the videos of Anonymous: Cloud activism, living networks, and political mimesis. *The Fibreculture Journal*, *26*, 85–107.

Fish, A., & Follis, L. (2015). Edgework, state power and hacktivists. *Hau: Journal of Ethnographic Theory*, *5*, 383–390.

Foucault, M. (2002). What is critique? In D. Ingram (Ed.), *The political* (pp. 191–212). Malden, MA: Blackwell.

Fuchs, C. (2013). *Social media: A critical introduction*. London, UK: SAGE Publications.

Garfinkel, H. (1956). Conditions of successful degradation ceremonies. *American Journal of Sociology, 61*, 420–424.

Giddens, A. (1991). *Modernity and self-identity: Self and society in the late modern age*. Stanford, CA: Stanford University Press.

Goffman, E. (1959). *The presentation of self in everyday life*. Garden City, NY: Doubleday.

Goffman, E. (1963). *Stigma: Notes on the management of spoiled identity.* London, UK: Penguin Books.

Goffman, E. (1967). *Interaction ritual; Essays on face-to-face behavior*. Garden City, NY: Doubleday.

Graham, D. (2015, October 5). Edward Snowden says he'd go to prison to come home. *The Atlantic*. Retrieved from http://www.theatlantic.com/politics/archive/2015/10/edward-snowdens-prison-offer/409075/

Greenberg, A. (2015, March 30). DEA agent charged with acting as a paid mule for Silk Road. *Wired*. Retrieved from http://www.wired.com/2015/03/dea-agent-charged-acting-paid-mole-silk-road/

Harding, L. (2014, February 1). How Edward Snowden went from loyal NSA contractor to whistleblower. *The Guardian.* Retrieved from http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract

Irwin, J. (1985). *The jail: Managing the underclass in American society*. Berkeley, CA: University of California Press.

Jordan, T., & Taylor, P. (2004). *Hacktivism and cyberwars*. London, UK: Routledge.

Keen, A. (2015). *The Internet is not the answer.* New York, NY: Atlantic Monthly Press.

Kelly, M. (2009). *The political philosophy of Michel Foucault*. New York, NY: Routledge.

Kelty, C. (2008). *Two bits: The cultural significance of free software*. Durham, NC: Duke University Press.

Kubitschko, S. (2015). Hackers' media practices: Demonstrating and articulating expertise as interlocking arrangements. *Convergence, 21*, 388–408.

Ludlow, P. (2013, January 13). What is a "hacktivist?" *The New York Times*. Retrieved from http://opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist/

Menn, J. (2011, February 5). Cyberactivists warned of arrest. *Financial Times*. Retrieved from http://www.ft.com/cms/s/0/87dc140e-3099-11e0-9de3-00144feabdc0.html#axzz3xF2rVlYL

Mitnick, K. (2012). *Ghosts in the wires: My adventures as the world's most wanted hacker*. New York, NY: Back Bay Books.

Nemer, D., & Freeman, G. (2015). Empowering the marginalized: Rethinking selfies in the slums of Brazil. *International Journal of Communication, 9*, 1832–1847.

Nothhaft, H. (2016). The dream of enlightenment within digital reach? Concepts of modern democracy. In W. T. Coombs, J. Falkheimer, M. Heide, & P. Young (Eds.), *Strategic communication, social media, and democracy* (pp. 65–83). New York, NY: Routledge.

O'Hehir, A. (2014, October 23). Laura Poitras: "I knew this was going to piss off the most powerful people in the world." *Salon*. Retrieved from http://www.salon.com/2014/10/23/laura_poitras_on_snowdens_total_preternatural_calm/

Picone, I. (2015). Impression management in social media. In R. Mansell & P. H. Ang (Eds.), *The international encyclopedia of digital communication and society* (pp. 469–476). Oxford, UK: Wiley-Blackwell.

Reitman, J. (2012, December 7). The rise and fall of Jeremy Hammond: Enemy of the state. *Rolling Stone*. Retrieved from http://www.rollingstone.com/culture/news/the-rise-and-fall-of-jeremy-hammond-enemy-of-the-state-20121207

Risen, J., & Poitras, L. (2014, May 31). NSA collecting millions of faces from Web images. *The New York Times.* Retrieved from http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html

Russia Today. (2014, December 6). Snowden movie picks up top docu award. Retrieved from https://www.rt.com/news/212119-citizenfour-snowden-docu-award/

Sauter, M. (2014). *The coming swarm*. New York, NY: Bloomberg Press.

Shelby, T. (2015). Impure dissent: Hip hop and the political ethics of marginalized black urban youth. In D. Allen & J. Light (Eds.), *From voice to influence: Understanding citizenship in the digital age* (pp. 59–80). Chicago, IL: University of Chicago Press.

Thomas, D. (2003). *Hacker culture*. Minneapolis, MN: University of Minnesota Press.

Tsing, A. (2004). *Friction: An ethnography of global connection*. Princeton, NJ: Princeton University Press.

Urbina, I. (2014). Social media, a trove of clues and confession, *The New York Times*. Retrieved from http://www.nytimes.com/2014/02/16/sunday-review/social-media-a-trove-of-clues-and-confessions.html?_r=0

U.S. Attorney's Office for the Southern District of New York. (2012, March 5). Criminal complaint. *United States v. Jeremy Hammond*. Retrieved from https://ia601001.us.archive.org/8/items/322817-jeremy-hammond-federal-complaint/322817-jeremy-hammond-federal-complaint.pdf

U.S. District Court for the Northern District of California. (2015). Affidavit of special agent Tigran Gambaryan in support of criminal complaint. *United States v. Carl M. Force IV and Shaun W. Bridges*, March 25, 2015 (filed).

U.S. District Court for the Northern District of Texas. (2012). Grand jury indictment. *U.S. v. Barrett Lancaster Brown*, April 12, 2012.

U.S. District Court for the Northern District of Texas. (2014). Sentencing hearing transcript. *U.S. v. Barrett Lancaster Brown*, December 16, 2014.

U.S. District Court for the Southern District of New York. (2014). Sentencing memorandum on behalf of Jeremy Hammond. *U.S. v. Jeremy Hammond,* April 16, 2014.

U.S. District Court for the Southern District of New York. (2015). Trial transcript. *U.S. v. Ross William Ulbricht*, January 20, 2015.

We steal secrets: The story of Wikileaks [film]. (2013). Alex Gibney, director. London, UK: Focus Films.

White House, The. (2015, June 9). A response to your petition on Edward Snowden. *The White House.* Retrieved from https://petitions.whitehouse.gov/response/edward-snowden

Wolgar, S. (2000). Social basis of interactive social science. *Science and Public Policy, 27*(3), 165–173.

Zadrozny, Brandy. (2015). Crime-scene selfies: Generally a bad idea. *The Beast*. Retrieved from http://www.thedailybeast.com/articles/2015/02/09/crime-scene-selfies-generally-a-bad-idea.html