HACKER, HOAXER, WHISTLEBLOWER, SPY

THE MANY FACES OF ANONYMOUS

Gabriella Coleman

VERSO
London • New York

Epilogue: The State of Anonymous

> "I have grown to love secrecy. It seems to be the one thing that can make modern life mysterious or marvelous to us. The commonest thing is delightful if only one hides it."
>
> Oscar Wilde

> "The political education of apolitical technical people is extraordinary."
>
> Julian Assange

The period described in this book may seem to many to represent the pinnacle of Anonymous activity: their support role in the various movements that constituted the Arab Spring; the high-profile media attention garnered by the gutsy LulzSec and AntiSec hacks; the ever growing commitment to domestic social justice issues seen in engagements against rape culture and police brutality.

Unsurprisingly, this impressive flurry of protest activity was met with similarly impressive law enforcement crackdowns. Throughout Europe, Asia, Australia, and the Americas, law enforcement officials detained over one hundred Anonymous activists—including many of the figures profiled in this book: Jeremy Hammond and John Borell in the United States, and Ryan Ackroyd and Mustafa Al-Bassam in the United

Kingdom. Others arrested were geeky activists whose "crime" had been to simply channel a small portion of their computer resources toward DDoS campaigns organized by Anonymous in an effort to collectively shame financial organizations, such as PayPal when they caved to government pressure and terminated all services to the embattled whistleblowing organization WikiLeaks.

Compared to every other nation in the western world, the United States acted with particular aggression in its legal pursuit of Anonymous activists and hackers: jail sentences were not only much longer but were also accompanied by astronomical fines. American Anonymous activists such as Jeremy Hammond, and even affiliated strategists such as Barrett Brown, faced stiff sentencing in the wake of the Stratfor hack (more on his case momentarily). Once released, these individuals will continue to pay for their actions as they struggle with the heavy financial debts imposed by their sentencing.

These punishments, combined with the knowledge that the FBI had succeeded in using Sabu, a core Anonymous figure, as their eyes and ears for months, caused mistrust, suspicion, and fear to intensify among Anons. Lips tightened. Hacker crews, who had always assumed snitches were lurking in every corner, became even more paranoid and reacted by paring down membership and enhancing operations security. Crucially, they also toned down their braggadocio.

In 2013 Anonymous seemed to have mostly shifted away from computer infiltration activities. But while such actions slowed down, they continued nonetheless, albeit more quietly. Italian Anons continued to hack and DDoS, and one of the most prolific hacking-oriented Anonymous outfits, Operation Green Rights, hacked into and defaced dozens of environmentally negligent companies like Monsanto (for reasons that are not entirely clear to me, they never attracted much media attention or resulting scrutiny). Undoubtedly, by 2014 and continuing well into 2015 Anonymous's most visible

activities in North America and Western Europe tended toward publicity rather than direct action, with a firm emphasis on consciousness-raising ops. In the UK, Operation Death Eaters has sought to bring attention to the problem of child sex trafficking and cover-ups of pedophilic activity by some of the country's most powerful figures. In the United States, OpFerguson commenced to support and publicize protest activities after a police officer shot and killed an unarmed African American teenager named Michael Brown. OpISIS, which in many ways aligns with the interests of Western state powers, is mandated to identify and publicize ISIS Twitter accounts and websites so they can be removed from the web.

The type of spectacular hacks that had been Anonymous's direct ticket into mainstream awareness continued to make headlines—but most were instigated by other, unaffiliated hacker groups. Most of these entities had little in common with the Anonymous hackers who aimed at social justice or politically salient direct action. In fact, many of them were directly antagonistic to such agendas. In 2014, Sony Pictures Entertainment became the target of hackers when the mysterious Guardians of Peace exfiltrated a massive amount of sensitive company information, allegedly in retaliation for the planned release of a film lampooning the North Korean government. The hackers released the cache to the public: everything from pre-screening copies of forthcoming films to internal briefings and company emails. During the 2014 holiday season Sony was targeted again, when Lizard Squad—a group reminiscent of LulzSec but lacking an overt political agenda—entertained its Twitter followers by disabling the PlayStation Network with a massive DDoS attack on Christmas day. In 2015 pro-ISIS hackers known as the CyberCaliphate hijacked a US government Twitter account in January, a *Newsweek* account in February, and even gained complete control of a French TV network in April.

But appearances can be deceptive. Hacking under the name Anonymous hadn't ceased; it was merely less visible. In Latin

America and parts of Asia, Anonymous hackers, most of whom had been active for some time, continued to worm their way into computer systems. One of the more prolific crews, LulzSec Peru, performed dozens of operations, including commandeering the Twitter account of Venezuela's president, Nicolas Maduro, and hacking documents from the Chilean Air Force. Their most momentous hack materialized on February 11, 2014, when they publicly released email evidence of Peruvian government corruption. As reported by Frank Bajak of the Associated Press, the leaked emails from the Peruvian Council of Ministers network sparked a "national uproar" and "fueled accusations that top Cabinet ministers have acted more like industry lobbyists than public servants. That helped precipitate a no-confidence vote … that the Cabinet barely survived."[1]

While this hack was enough to draw the attention of English-speaking journalists, for the most part the Western media has remained oblivious to most foreign Anonymous activity. Of course, even journalists willing to cover these events are typically ill-equipped to do so. Language barriers combined with the difficulty of gaining access to hackers—more reticent than ever after a spate of arrests—made the type of reporting common during the LulzSec period much harder to replicate.

The lack of media attention might be less a sign that Anonymous has slowed down, and more a sign that it has simply sharpened its survival skills. While thanks to their own publicity efforts we know that AntiSec and LulzSec were forces to be reckoned with, their excessively public character was ultimately their greatest weakness. It can be difficult to weigh the pros and cons inherent to each approach. By garnering attention, LulzSec and AntiSec were able to showcase their causes, and also inspire others to join up or follow their lead. But the longer these stable teams labored under the intense watchful scrutiny of the media, the public, and especially the state, the more susceptible they became to capture. With every public hack and with every taunt—especially with

many of them directed at law enforcement—the pressure to identify and snuff them out grew.

But as is the case with any nascent political movement whose organizational styles and approaches are untested, Anonymous's flirtations with fame and other rough-and-tumble tactics were necessarily experimental. It is no wonder the outcomes tacked between spectacular success and equally spectacular failure. With inevitable missteps come collateral damage, but activists can learn from their own blunders and also those of others.

And it seems that at least some have been paying attention. Take, for instance, the 2014 hack against Gamma Group, a British spyware firm devoted to selling "advanced technical surveillance [and] monitoring solutions"[2] to governments—including dictatorial and repressive regimes known to use those tools against dissenters and activists. In 2011 the software firm gained notoriety when WikiLeaks published one of the company's promotional videos alongside brochures and presentations that demonstrate how their software can be used to infect a computer.[3] Soon after, two security researchers suggested it was possible the Bahraini government had used this method to surreptitiously deliver software called FinFisher to local activists via email attachments. (In response Gamma claimed the software might have been stolen, as company representatives insisted they never sold FinFisher to Bahrain.)[4]

On August 3, 2014, a hacker calling himself Phineas Fisher (Phineas being the name of a seer from Greek mythology) appeared out of the blue and announced on various social media platforms that he had broken into Gamma's computer systems and was releasing forty gigs of FinFisher-related data. The wide-ranging documents included technical material (software blueprints, source code, documentation, use analysis) along with client lists, price lists, tutorials, and more. Among other revelations, the Phineas Fisher hack helped fortify the evidence that the Bahraini government had used FinFisher to target activists.[5]

In a statement released alongside the leak, Phineas Fisher exhorted his fellow hackers to "hack back," and gave them some pointers. *Hack Back!: A DIY Guide for Those Without the Patience to Wait for Whistleblowers* opened with the following advice:

> As long as you follow common sense like never do anything hacking related outside of Whonix, never do any of your normal computer usage inside Whonix, never mention any information about your real life when talking with other hackers, and never brag about your illegal hacking exploits to friends in real life, then you can pretty much do whatever you want with no fear of being v& [vanned: a term for being raided or detained by law enforcement].[6]

Although Phineas Fisher did not align himself explicitly with Anonymous, his hack embodied the group's spirit, and was without a doubt indebted to the particular leaking style LulzSec and other Anonymous groups had inaugurated. (Phineas Fisher has also revealed he is a connoisseur of the lulz when he wrote in *Hack Back!*: "It was only after failing to fully hack Gamma and ending up with some interesting documents but no copy of the FinSpy server software that I had to make due with the far less lulzy backup plan of leaking their stuff while mocking them on twitter.")[7] In the context of a dramatic surge in leaking and whistleblowing activity in recent years, most notably by brave citizens like Chelsea Manning and Edward Snowden, the Anonymous mode of leaking was distinctive for its risky direct-action component: rather than leaking files entrusted to them, they infiltrated the networks of corporations and governments in order to exfiltrate information from security and intelligence firms.

Where Phineas Fisher diverged from the likes of LulzSec and AntiSec was not in method or choice of target, but rather in demonstrating far more care, precision, and caution than Anonymous ever did. Furthermore, rather than use his time in

the limelight for self-promotion, Phineas Fisher dumped the data onto Twitter and reddit, worked to draw attention to the material for five days, and then simply vanished.

That is, until he reemerged on July 5, 2015, to claim ownership for a similar hack—this time targeting another, even more reviled, supplier of cyber weapons called Hacking Team. The Milan-based software and security company sells what it describes as "offensive solutions" to a range of customers, from the FBI to the US Army.[8] Phineas Fisher this time gained access to their Twitter account, changed the company's name from Hacking Team to Hacked Team, and adopted their identity to make an announcement: "Since we have nothing to hide, we're publishing all our e-mails, files, and source code [link]."[9] Prior to the hack, these mercenary technologists had done everything possible to conceal the specific nature of their services, dealings, and customers. Thanks to the massive 400 gigabytes of data released, all of that has changed. Like GammaGroup, Hacking Team publicly maintained that it never sold goods to repressive regimes. Now we know otherwise. According to the leaked data, it did sell to such governments without any qualms and engaged in many other questionable practices, including stockpiling and hoarding critical software vulnerabilities—including two in the ubiquitous Adobe Flash player—that could be used against millions of Internet users.

By way of proving he was Phineas Fisher (and also to suggest that more was to come) he tweeted from the account he had previously set up to mock Gamma Group ("GammaGroupPR"): "gamma and HT down, a few more to go :)."[10] He also relinked to his *Hack Back!* manifesto/DIY manual. The maxims contained in Phineas Fisher's manual are not new. They have been long known and embraced in hacker circles, including among the hacker elite of Anonymous (a number of whom, it must be said, were never caught and remain out of jail). Still, given the difficulty in implementing security measures, and the arrests of Anonymous hackers, one might recognize a certain

prudence in repeating the core principles time and again. And much in the same way that Phineas Fisher has beseeched his fellow hackers to practice exceptional security, Anonymous, following the Sabutage of 2012, now constantly cautions its newcomers to take security seriously. "If you're a newblood," Anon2earth tweeted, then "chill—sit back and lurk. Don't get into any ops unless you know what the fuck you are doing. Protect yourself."[11] In Anonymous circles, security advice and admonishments are now part of the routine backdrop of everyday conversation.

Far from being empty slogans, it seems these lessons have been heeded not only by hackers like Phineas Fisher, but also within the ranks of Anonymous. Take for instance OpCyberPrivacy—a general campaign opposed to Western surveillance laws such as Canada's Bill C-51, minted in 2015 and criticized by academics, lawyers, journalists, and dozens of civil society groups for granting undue power to law enforcement and intelligence organizations. At first, Anons attempted to attack the bill through publicity alone, but failing to make headway or obtain media traction, they resurrected an Anonymous classic tactic: the DDoS.

On June 17, 2015, Anonymous disabled dozens of Canadian government websites, including that of the Canadian Security Intelligence Service (CSIS) and the departments of Justice, Industry, Trade and Development, Natural Resources, and Foreign Affairs. More significantly, they managed to disrupt digital communications by intentionally hitting an email server. The campaign secured extensive coverage. According to *The Globe and Mail*, "It was the most high-profile cyber attack in this country since Chinese state-backed hackers broke into Canada's premier scientific research agency last year."[12] Shortly after the campaign, one of the organizers explained to me that "the core work group" had been collaborating closely "now for about seven months," on various ops: "from hunting Ferguson cops, Ukrainian revolution, Ku Klux Klan fuckery, pedophile hunts to privacy." Some of the Anons

were newcomers, while many of the core group had been around for many years. In marked contrast to the December 2010 Operation PayBack against PayPal, which resulted in the arrest of a slew of participants, he insisted security was such a priority that one of their goals was to avoid all collateral damage—anything that could be used by law enforcement to escalate their response. He concluded the chat by proudly noting there had not been any "[security] fails as of yet. Which is nice." Later, he informed me we had chatted in the past, but he had used a different nickname—and explained that from here on out names would be treated like burner phones: tossed away periodically, so that when an activist appears anew he will be, in essence, a different Anon, and one harder to connect to any previous operation.

Without the arrests of 2011 and 2012, it is hard to imagine such careful measures being put into place—and it also remains to be seen just how effective they will be. It seems that many in Anonymous are still uncertain about just what they can get away with—and what, exactly, is at stake. Much of this evaluation will hinge upon the treatment of those already arrested and their legal fate.

In the case of the PayPal14, most of the defendants narrowly escaped jail time. Eleven of the thirteen defendants pleaded guilty to a felony and a misdemeanor (felony charges were subsequently dropped since they followed the stipulations outlined in the plea deal). Two other defendants were respectively sentenced to three and four months in halfway homes, which allowed them to avoid felony sentencing. All thirteen had to pay $5,600 in restitution to eBay (formerly PayPal's parent company), and those that could not afford to pay in one lump sum were required to pay a monthly fine of $100. The fourteenth member of the bunch, Dennis Owen Collins, was one of the most dedicated members of AnonOps (he features in this book as "Fred" and "Owen," see index). While completing one year of house arrest, he passed away on July 16, 2015, at the age of fifty-four, after fighting a battle

with the debilitating and chronic pulmonary disease he suffered from most of his adult life.

Of all the American cases concerning Anonymous, one stands in a class of its own: that of Barrett Brown. On January 22, 2015, in a packed Dallas courtroom, Judge Samuel Lindsay handed down a stiff sentence to the journalist and rabble-rousing activist. Brown, who at the time of sentencing had already been behind bars for more than two years, received an additional thirty-five months in jail and a restitution fee of nearly $1 million to be paid to the hacked intelligence firm Stratfor. Originally facing seventeen charges, after taking a plea bargain which reduced the possible sentencing to eight years, he was ultimately only convicted of three crimes: making threats against an FBI agent, obstruction of a search warrant, and assisting the Anonymous hackers who infiltrated and gutted the Austin, Texas–based intelligence company.

What was most exceptional—and most questionable—about the whole affair was the judge's allegation that Brown had "more than merely reported the hackers' activities" but had more accurately helped organize them: "The Court concludes that Mr. Brown collaborated with and supported the hackers identified targets [*sic*], provided advice, strategized and assisted in organizing hacker activities."[13]

Yet the fact remains that Brown wasn't a hacker, nor was he officially charged with any hacking crimes. Brown's role in Anonymous was that of an avid strategist. There was no solid evidence he coordinated—much less partook in—the actual infiltration of Stratfor, which took place in December 2011. Brown was mostly interested in the emails, though he did post a link to credit card numbers stolen by Anonymous hackers and at one point faced a criminal charge for doing so. Out of all seventeen counts he originally faced, this one was the most controversial: he had not stolen or used the credit card information but was simply reposting a widely circulated link from one chat room to another. While the charge was dropped in March 2014, the judge nevertheless agreed with

the prosecution's arguments that linking to the stolen data had aided the hackers, and thus must be considered relevant to the broader sentencing. It was "more than just the mere posting," reasoned the judge. "It goes to his involvement with the others who were involved in this same activity."[14] Thus even without the charge, the severity of Brown's sentencing was increased.

This legal contortion and murkiness clearly chills speech—creating a situation where other journalists would be less inclined to share links, fearful that such activity could be seen by a court as aggravating a crime (in the wake of the ruling, journalist Quinn Norton announced she would no longer report on breaches, infosecurity, or hackers for fear of similar government retribution.)[15] Like so many hackers, whistleblowers, journalists, and hacktivists who have risked everything to stand for press freedom and accountability, Brown is now paying a steep price; the sentence speaks to the state's willingness to prosecute not only politically motivated hackers, but also geeks and journalists like Brown who work closely with them.

The harsh legal treatment of US-based activist hackers and supporters like Hammond, Brown, and others is at the center of an ongoing case as I write this epilogue. On July 15, 2015, a British hacker named Lauri Love was arrested in his home country and now faces extradition to the United States, where he has been charged under the Computer Fraud and Abuse Act in New Jersey for allegedly hacking into the NASA, the US Army, and the US Federal Reserve as part of Anonymous's OpLastResort, catalyzed by the suicide of hacker Aaron Swartz. Love's supporters are doing everything they can to stop his extradition, concerned that if he is shipped off to the United States—where punishments are much stiffer—he might also take the tragic path chosen by Swartz. "Extraditing Lauri Love to the United States," they insist, "would be a gross violation of both his human and civil rights."[16]

The state has long relied on prosecutorial overreach and repression to create a climate of fear capable of squashing political movements, or at least constraining their growth. It

is perhaps remarkable, then, that so many geeks and hackers have been not only undeterred by the law enforcement response, but instead galvanized into action. The revelations provided by Snowden, in particular, have been experienced by geeks and hackers as a historic and urgent wake-up call: they have given scores of renewed focus and vigor, reenergizing the pursuit of pro-privacy agendas through the development of encryption tools.

Since their arrests, many ex-members of Anonymous, LulzSec, and AntiSec have continued to contribute avidly to this privacy movement. During the summer of 2015, Donncha O'Cearbhaill was chosen by Tor, the premier encryption project, to work as a summer intern under the guidance of one of the project's long-term developers. During an interview with the organization, he was asked, "Who are your heroes—if you have any—in internet freedom software?" O'Cearbhaill replied by honoring those he worked with directly and the general community of hackers: "The work of many people in the Internet freedom community inspires me. I'm particular grateful to people such as Edward Snowden, Julian Assange, and Jeremy Hammond who have made massive sacrifices to try to bring light to the expanding surveillance state. I'm inspired by the free software developers and advocates everywhere who continue trying to doing something about it."[17] Mustafa Al-Bassam, still an intern at Privacy International, has diversified his contributions. After the Hacking Team files were released to the public, he hosted them on a site, ensuring they would remain available for download. The files were in high demand; his site got pounded for days, prompting him to work around the clock to keep it up. Al-Bassam also collaborates with security researchers and other ex-Anons, including Darren Martyn, through an informal hacker think tank called LizardHQ. So far they have drawn attention to questionable surveillance tools and their vulnerabilities, including Hola (a VPN with 10 million users that also, it turns out, contains a backdoor for recruiting users' computers into botnets);

E-Detective (a lawful intercept product that is used by the Chinese military and over 100 international police forces); and Impero (spyware used by a portion of UK schools to snoop on students). He explained to me that the purpose of LizardHQ activities is to "expose the vulnerabilities that allow this to happen so that people can make informed decisions about the systems they participate in that disregard their civil liberties … We don't coordinate vulnerability disclosure with vendors who develop spyware nor inform them beforehand, because doing so would set a bad precedent of security researchers cooperating with spyware vendors."

As confirmed by numerous polls and studies, since Snowden the broader American public is more concerned than in the past about preserving privacy.[18] And the United Nations has also weighed in; its Office of the High Commissioner released a report defending the democratic sanctity of encryption, for its ability to "provide the privacy and security necessary for the exercise of the right to freedom of opinion and expression in the digital age."

And yet, as the court of public opinion shifts, law enforcement and other government officials are responding predictably—and as they have done for decades—by demonizing both encryption technologies and associated ideals of anonymity. In response to pressure from users, proprietary software firms like Apple and Google have gone to great lengths to advance user security—prompting an insistent antagonistic response from the FBI and other law enforcement agencies that corporations instead have a duty to "prevent encryption above all else." In October 2014, the FBI director gave an alarmist and scathing speech about privacy at the Brookings Institution in Washington, DC: "With Going Dark, those of us in law enforcement and public safety have a major fear of missing out—missing out on predators who exploit the most vulnerable among us … missing out on violent criminals who target our communities … missing out on a terrorist cell using social media to recruit, plan, and execute an attack."[19]

There is, in other words, now a pitched civil liberties battle over the future of privacy and anonymity. This fight, of course, is certainly not new. But only recently has it escaped the rarefied habitats of legal theorists, policy makers, technologists, and academics and entered into the hands of a more general swath of technology collectives, lawyers, journalists, filmmakers, hackers, software and hardware developers, NGOs and concerned private citizens. Akin to the way that free speech ideals pierced public consciousness during pitched political battles—such as those waged in Spokane by the Industrial Workers of the World in the early 1900s or by the Berkeley free speech protests in the 1960s—grassroots privacy initiatives appear to be approaching a critical mass.

Anonymous's position within this newly minted grassroots privacy movement merits further examination. Of course, given its namesake and symbolism, Anonymous's very existence affirms a commitment to the values under siege. But having an entity like Anonymous so closely linked to a social movement is in many ways a double-edged sword: while Anonymous can popularize issues and draw in membership, it can also draw criticism from detractors. Given its proclivity to incite contention, this is to be expected. There is no way to whisk away the controversies Anonymous stirs up, and even when its intention is to do just that, the results can be unpredictable, unproductive, and in some cases even harmful.

Nevertheless, more than any other political movement, past or present, Anonymous provides the ideal case study through which to probe the workings, benefits, contradictions, and limitations of applied anonymity-in-action. And as this privacy movement coalesces, I have observed a distinct tension among those who believe in anonymity as a politically useful tool. Even as many leftist and liberal advocates unequivocally support a right to encryption, they also sometimes express a deep discomfort about the use of secrecy among activists, the role of anonymity in general, and the function of Anonymous in particular. To put it slightly differently, many

are uncomfortable with the way Anonymous, and anonymous actions more generally, lack accountability or, in a more trenchant version of the criticism, demonstrate basic cowardice. One academic bluntly expressed his discomfort with anonymity recently by declaring "the opposite of anonymity is responsibility."

While the association between anonymity and irresponsibility is far more complex than that statement implies, it is undeniable that a core feature of intentional cloaking is the ability to evade attribution. Privacy scholar Helen Nissenbaum has defended anonymity on these very grounds: "the value of anonymity," Nissenbaum asserts, "lies not in the capacity to be unnamed, but in the possibility of acting or participating while remaining out of reach, remaining unreachable."[20]

While limited forms of secrecy and shelter from legal repercussions are vital for Anonymous, the arrests of LulzSec and other participants have made it clear to current Anons that anonymity is never absolute. Many Anons are aware of the risk—and thus act always with a sense of their actions' future consequences: framing their activity as though it were certain to be uncovered, even as they hope it might not be. And, in some instances, Anons eschew even the attempt at this stringent, technical, security-motivated anonymity—instead taking up only the social anonymity that allows them to interact with other Anons in an egalitarian manner. One member of the PayPal 14, Keith Wilson Downey, acknowledged this predicament when rationalizing his participation in Operation Payback: "As a proponent for the freedom of information for over a decade, I decided I was going to do more than just talk. So on December 9th, 2010 I downloaded LOIC, connected to the hive and joined the protest against PayPal. It's also worth noting that I decided not to cover my tracks as I considered this to be a legitimate protest that was worth the risk. Which is a decision that has changed my life for the three years that followed."[21] For Downey, anonymity wasn't a shell to escape attribution, but a frame from which to enable action.

It is difficult to boil down the workings of anonymity within Anonymous to a single logic: whatever formulation you come up with, it can always be adopted and repurposed, in different ways and towards different ends, by whoever wants to use it. It can never be owned, much less controlled, effectively because any attempt to do so will change the thing into something other than anonymous; the ideal itself is thus, in some ways, incorruptible (or endlessly corruptible)—always outside the reach of power, even if those temporarily experiencing it, or who believe themselves to be experiencing it, can themselves be grasped. Nevertheless, Anonymous has clearly enabled a new political subject position, one where the point is to exceed "talk" as Downey put it, one where *actions* matter, and actions can be evaluated, but the identities behind them—even when they are identifiable and subject to prison—are acknowledged by all involved to be less important than the actions they perform. In this way, even when the individuals are named, the value of the anonymity they once believed they enjoyed is preserved in the actions it enabled them to perform. Belief in the idea of Anonymous is enough to motivate action, even if full anonymity is not the goal or is unachievable.

Although Anonymous participants are veiled by a pseudonym whenever they act in public, it is also vital to emphasize that most of the actions themselves are in no way carried out in secrecy. These activists organize on public chat channels, issue press releases, and announce their causes and offer reasoning in dramatic videos. They are also typically in direct contact with local non-Anonymous activists and journalists. During the first few days of OpFerguson, for instance, CNN was in contact with participants on IRC, attempting to lure them into live TV appearances. It is hard to imagine a journalist would be able to secure similar upfront access with terrorists or black hat criminal hackers who seek—at all costs—to evade contact with the state and the public at large. Most Anons, in other words, are not hiding out in the Internet's equivalent of the Tora Bora caves, scheming in total darkness. They are acting

primarily in the light of day, albeit with a measure of safety—just enough to allow them to act at all.

Typically, it is also straightforward to associate particular operations with specific groups, Twitter accounts, IRC networks, or individuals. By way of an example, take again OpCyberPrivacy. Soon after the group behind the OP completed a series of DDoS attacks in protest of Canada's Bill C-51, another Anonymous hacker known as ro0ted announced that he had hacked a Canadian government website. He released employee names and credentials. Initially, journalists pinned the hack to the OpCyberPrivacy Anons. But its participants, who had nothing to do with the hack—and in fact vehemently criticized it as irresponsible for its violation of privacy—immediately reached out to the journalists to seek a correction. As any cursory investigation would have revealed, ro0ted did indeed claim involvement with Anonymous. But not with OpCyberPrivacy, rather with the Anonymous cyberguerrilla network.[22] Most of the articles were quickly amended, and a characteristic of Anonymous was made clear to those paying attention: responsibility can still be sought even among those with a modicum of operational anonymity.[23]

Even if most actions performed under the mantle of Anonymous can be connected to some responsive entity, many observers still express concern about accountability when there is no ultimate recourse to legal identity. One question frequently lobbed my way is: If Anonymous is clandestine, how can they be answerable to the communities they work with?

Yet it is worth considering to what extent such responsibility is possible in communities that are ostensibly transparent and accountable. To probe this further, consider the field of journalism—often posited as the quintessentially transparent enterprise. Journalists publish stories with their legal names and the credibility of news media depends on their publishing facts not lies. And yet it is accepted as a necessity—even a sacrosanct right—that journalists can selectively rely on

anonymous sources as well, particularly when access or information could not be provided without it.

Still journalists do on occasion commit acts similar to what Anonymous also faulted for: publicizing the names of sensitive individuals and thus putting them in harm's way—doxing. This tactic (understandably) is one of Anonymous's most controversial and at times deeply unsavory practices. As this book has explored, doxing often ruffles the feathers of others within Anonymous, particularly when someone releases names of innocent bystanders or incorrectly attributes an action. This happened with OpFerguson when an Anonymous Twitter account, TheAnonMessage, released the name and photos of a police officer in the mistaken belief that he was responsible for gunning down Michael Brown.

Even if journalists are never accused of doxing per se, the effect is at times the same—and it is a mistake made not only by tabloids or news sites like Gawker, whose founder famously boasted, "I have a simple editorial litmus test, which is: is it true, and is it interesting?"[24] In 2014, the same year Anonymous incorrectly doxed the Ferguson police officer, the most conspicuous dox of the year was not the handiwork of Anonymous, but rather *Newsweek*.

To much fanfare, the magazine relaunched its print edition in March 2014 with a major cover story: their journalists had purportedly determined the real-life identity of Satoshi Nakomoto, the famously pseudonymous founder of the cyptocurrency Bitcoin. *Newsweek* insisted that the screen name was in fact not entirely pseudonymous: that Dorian Nakamoto, an elder Japanese-American engineer living in Southern California, was the elusive man and mind behind the popular digital currency. The investigation, story, and aftermath were nothing short of deeply intrusive—taking the form and logic of a hacker-instigated dox. The investigating journalist, Leah McGrath Goodman, posted a picture of Nakamoto's house, replete with a legible street address and a car's license plate. Tracking him down afterwards became a trivial affair. And this

information was further hedged by a thicket of private details about his finances, health, and marital woes—all of it aired to millions of Americans. Subsequently the *Los Angeles Times* participated in a "Bitcoin chase" alongside other news outlets, in which they confronted Dorian at his home, ambushed him with photographers, followed him into an elevator for questioning, and later mocked him in print for emerging from his home into the scrum and offering to allow one of the mobbing reporters to interview him in exchange for a free lunch.

Countless experts, journalists, and observers faulted *Newsweek* for the flimsy evidence used to justify the identification; yet in spite of near universal condemnation by critics, *Newsweek* to this day stands by the piece with the following weak public interest defense: "We recognized a public interest in establishing some core facts about Bitcoin and better informing those who might invest money in it."[25] Even if they had identified the correct person, the ethical justifications for prying open his life to the public at large would seem dubious. The founder of Bitcoin has repeatedly expressed his desire to remain anonymous; more importantly, his actions have not caused harm or wrongdoing, nor is it in any way necessary to acquaint oneself with the details of the private life of the founder to make sound "investing decisions" about Bitcoin, as the *Newsweek* editors suggest.

Of course, since *Newsweek* is a legally constituted and public entity, they can be sued—and in 2014 Nakamoto was said to be exploring this option. Yet it is almost impossible to sue a faceless collective for doxing, unless the perpetrator is first caught by the state or outed by their peers. For *Newsweek*'s potential mistake and violation of privacy, Nakamoto might eventually be rewarded some huge lump sum of money,[26] while an incorrectly doxed police officer was subject to death threats with no chance of reparation.

Juxtaposing these two cases evinces some important differences in the accountability of Anonymous, a camouflaged protest entity, and a known person or a public institution.

But other examples of journalistic inaccuracies and oversights have resulted in far more troubling collateral damage than anything Anonymous is typically capable of. While a faildox by Anonymous may recklessly endanger a handful of individuals, failed attribution that is uncritically repeated by mainstream media can potentially aid and abet decisions that alter the fates of entire nations. The most egregious and insidious journalistic lie of the last decade is so well known it barely needs mentioning: it occurred when the *New York Times* published a piece that uncritically parroted the government's position that Saddam Hussein was stockpiling weapons of mass destruction. As numerous critics have pointed out, this single article helped justify a costly and atrocious war in Iraq, a course of action no lawsuit or civil society response could hope to redress.

While this example may appear to be a one-off outlier in its extremity, many other mundane examples of harmful journalistic missteps premised on reckless claims-making can be flagged, often in relation to the domain of technological activism itself. Many British papers have published stories that smear Edward Snowden as a Russian spy—without even attempting to offer evidence. Julian Assange, so often accused of being irresponsible with his leaks, lambasted a *Guardian* reporter who published a sensitive internal password as a chapter heading in a book detailing his collaboration with WikiLeaks. According to Assange, it resulted "in the dumping of hundreds of thousands of State Department cables onto the Internet without the selective redactions that had been carefully prepared for them."[27] Assange had entrusted the password to select journalists with the express understanding that the material accessed needed to be carefully vetted before publication to avoid the inadvertent doxing of innocent people.

Finally, let's examine a case directly related to Anonymous, and one covered earlier in the book. In February 2012, at the height of Anonymous's public popularity—when Polish

politicians donned the Guy Fawkes mask to register dissent against a trade treaty—a *Wall Street Journal* writer named Siobhan Gorman painted the hacktivists as dangerous extremists. Anonymous "may have the ability within the next year or two to bring about a limited power outage through a cyberattack," she wrote. The proof was embarrassingly scanty, boiling down to a single sentence: "Gen. Keith Alexander, the director, provided his assessment in meetings at the White House and in other private sessions, according to people familiar with the gatherings."[28] The evidence was not only flimsy, but it was so out of character with Anonymous's public behavior that the article fell flat on its face. But had it stuck, it could have invalidated the efforts of an entire political movement to contribute positively to a variety of social causes.

Anonymous at times makes mistakes, and journalists do too. But when mistakes are made by a reputable paper, the usual response is not to denounce the entire field of journalism or even the entire publishing house, but rather the particular article, author, or editor in question. Why should it be any different for Anonymous? Particular mistakes made by Anonymous or the *New York Times* or *Newsweek* all merit a sharp rebuke. And this is precisely what occurred in the case of OpFerguson when TheAnonMessage released an incorrect name. I was watching in real time on IRC when this participant was gearing up to release the name of the police officer. It was early in the morning and most members of the operation not around or idling. Usually doxing operations occur privately and this was out of character because TheAnonMessage was acting whimsically without consulting the core team, which normally happens behind closed doors in private channels. Once he went public with the name—and it was clear that he got it wrong—almost every other member of the operation became infuriated and lambasted the Anon in question. One of his most vocal critics was Crypt0nymous, a respected video/media maker in Anonymous, who went on a tirade against @TheAnonMessage on Twitter.[29] He posted dozens

of messages about his shoddy and irresponsible work that, according to Crypt0nymous, was motivated by a desire for personal glory and fame. This sort of informal censure and condemnation may not be robust enough to right all wrongs but, nevertheless, informal drubbing mechanisms do modulate future activity, usually for the better.

The smattering of examples drawn from the field of journalism is not meant to justify the harmful consequences that cascade from Anonymous's doxing; two wrongs certainly don't make a right. It is merely a reminder that working under a regime of transparency alone does not guarantee accountability. Indeed, when reputable newspapers, like the *New York Times* or the *Wall Street Journal*, publish fibs or stories with scanty evidence the consequences can be far more negative than when an entity like Anonymous spreads them; those papers are seen as vehicles of objectivity and truth. Their reputations tend to be rock-solid and are hard to puncture. Anonymous's claims, on the other hand, are often treated, even by supporters, with some degree of skepticism.

Indeed, it is commendable that Anonymous signals the biases and perspectives that are inherent to all informational environments, whether they are due to cognitive limitations, informational overload, the inherent biases that are part and parcel of knowledge production, imperfect information, or outright manipulation. The fact that we know Anonymous is fallible is valuable in itself. They do not claim objectivity. They do not claim to be fair and balanced, but merely to be activists doing their best (or doing their best to be mischievous). Thus their failures are immediately prevented from doing too much harm because no one expects them to be 100 percent correct all the time in the first place, unlike a reputable agency like the *New York Times*.

Still, comparisons between Anonymous and journalism can only go so far. The scope of activity engaged in by Anonymous, an action-oriented political movement, is far greater than that of news media, mandated only to disseminate information.

While Anonymous is in many instances accountable, albeit pseudonymously, by operation group, in other instances their most radical, direct-action manifestations depend upon secrecy and anonymity even in relation to other Anons. The riskiest of direct-action activities, in particular, are often enabled and encouraged within secretive nooks, like the "cabals within cabals" described earlier in the book. Another use of secrecy aims less at security and more at maintaining a type of internal social harmony: Anons ostracize those who engage in social peacocking behaviors, often demanding that personal identity be sublimated not simply for personal security, but rather for reining in personal ego.

These two registers of obfuscation provide examples of what communication scholar Jack Bratich lauds as "minor popular secrecy," valuable for "providing a counter to a politics based on identity and representability."[30] Often, he suggests, attempts by social movements to demand visibility and representation function less to further their political demands and more to make them legible to state mechanisms of cooption or dismissal.[31] Noting the state "abhors a mask that is not its own," he suggests there is a massive power disparity at work in the way the state "demonizes" masks used by its citizens while always refusing to relinquish its own. As a result, he argues that leftist activists should reserve a limited but important place for secrecy. When activists chide all forms of secrecy in activism, they are inadvertently bolstering state power; their transparency demonstrates all their vulnerabilities for a masked opponent to exploit or coopt from a safe advantage.

What do activists gain by relying on minor and limited forms of secrecy, especially when fortified by an ethics of obfuscation used to encourage egalitarianism? And is it possible that the use of secrecy can be ethically justified when used by underdog political activist groups, and also be roundly condemned when used by those, such as states and powerful economic actors, who already exercise an advantage or

monopoly on power? When secrecy is used by nation states not only instrumentally but as a general and ever-expanding rule of operation—as is especially the case with intelligence agencies endowed with seemingly limitless technical and financial resources—its effects can often run counter to public interest.[32] Secrecy, on the other hand, affords resource-poor activists, like Anonymous, an ability to strike against the powerful. It levels the playing field. When used in a limited fashion, cloaking can alter the political landscape for the better, by enabling structural conditions capable of enabling principled action, rather than only principled deliberation and communication; it can also constitute a form of direct action in its own right. As Julian Assange has put it, "Cryptography is the ultimate form of non-violent direct action."[33]

And there are real costs to political inaction. When people privilege the liberal politics of debate, reform, and publicity above direct engagement in change, it is difficult to understand where, exactly, the change is expected to come from when the government opts not to listen. Our society champions transparency and civil debate. These mechanisms are often treated as the preferred way to create political pressure capable of pushing policy makers and lawmakers to initiate change. But while making information publicly available and open to debate is undeniably invaluable, for information to become truly politically meaningful, it sometimes needs to be made actionable—needs to be fashioned into a demand that cannot be ignored.[34]

Civil disobedience is one way of doing just that, and its exercise can serve as a model offering a greater swath of participants—those not served or offered a voice by conventional liberal politics, or minorities drowned out by unreflexive normative convention—a pathway by which to directly contribute to the political process. As Robin Celikates, a political theorist working on civil disobedience, has put it, "episodic, informal, and extra- or anti-institutional form of political action also allows citizens to protest and participate, when—as is

often the case in representative democracies—the official and regular institutional channels of action and communication are closed to them or are ineffective in getting their objections across."[35]

One may object to the use of civil disobedience by a minority. After all, is it possible their opinion is uncommon because it is undesirable? But this is a deceptive analysis. Civil disobedience, even when it works, only serves to draw attention to a position—one that must enroll many others into alignment, to constitute a much larger cause, if it is to change the broader consensus. The positions of individuals like Chelsea Manning, Jeremy Hammond, and Edward Snowden were little known until their courageous acts allowed their politics to be aired, and thus emulated by those in agreement. (There is likely at least one other leaker providing documents about the NSA to a variety of publishing platforms,[36] and Phineas Fisher was likely inspired by the Anonymous hacks against security firms.) Bravery of this nature, whether anonymous or not, challenges others to confront and sometimes shed their complacency. In other words, civil disobedience creates an environment where broader grassroots social movements can thrive.

Anonymous is a perfect example of this logic at work. Participants who dox, hack, or DDoS are in the minority. But in so doing they help to activate spectators and other participants—even those who disagree with their tactics or their outcomes.[37]

Yet the question of Anonymous's accountability is again raised by critics on this front—often critics who doggedly defend the use of civil disobedience by other social movements. Civil disobedience, they say, lacks legitimacy if it does not carry the stamp or seal of one's legal identity—if it is not legitimated by the risk of punishment. But as Molly Sauter has convincingly argued, this conception of civil disobedience is as narrow (and limited) as it is historically specific. It is a conception, she insists, "deeply rooted in concepts of Christian martyrdom and the moral superiority of nonviolent civil

disobedient over their opponents … in insisting that online political activists expose themselves to often extreme punitive state action because of their activism ensures that only those with the most extreme views and the least to lose (i.e., those with the least investment in society) will participate in these actions."[38]

As Anonymous continues to makes demands of the state, seeks to stamp out corruption, and connects with other activists to provide aid for political fights small and large, it is at work decolonizing deep-seated habits of subjectivity: it dares to work toward a collective good without the need for personal recognition and furthering a personal brand. Many of its participants are after all capable, law-abiding citizens who could, if they chose, seek some measure of personal, public glory in return for their contributions. Instead, they insist on the "right to opacity," as formulated by Edouard Glissant.[39] Masking, so often thought of only in negative terms—as shirking responsibility or hiding—can also enable a positive, constructive ethics of interacting and of being-in-the-world that runs counter to state, corporate, and colonial interests. Indeed this right embodies a series of defiant, principled refusals; a refusal to allow the state to track its citizens; a refusal to allow corporations to convert personal communications into profit or manipulate their personal desires; a refusal to capitalize off each other's labor; a refusal, in essence, to prevent a powerful idea—that we are and can be anonymous—from withering away.

July 2015

Acknowledgements

Even if a single concept is destined to fail at adequately conveying the vast and intricate geography fabricated by Anonymous activists, in writing this book I found myself consistently returning to one particular governing trope: the maze. Every attempt to traverse, understand, or describe a given state necessarily corrupted it, adding further entropic inputs which ensured a different experience for any who would participate within it or even simply watch. So, as it turns out, researching and writing about Anonymous was a thrilling but taxing enterprise. I spent years collecting too much material, attempting to build my own labyrinth that would allow me to chart a course through theirs. But when I set out to unravel the tangled threads, to find my way out of the collected stories, rumors, conversations, and secrets into some coherent and lucid narrative, I realized in horror that the gossamer material was disintegrating in my hands. I was lost in the nether regions between mazes, with no bearings and no way out. Thankfully, a host of friends, colleagues, strangers, and Anons helped me find my way, nudging me along on my journey and contributing to its ultimate manifestation as a book.

This project was long in the making. Its beginnings can be traced to a Killam Postdoctoral Research Fellowship I held at

the University of Alberta in 2006–7, and a fortunate introduction to Dr. Stephen A. Kent, who, in his work as professor of sociology, curates the largest academic Scientology archive in the world. In the midst of a frighteningly frigid winter, I dove into the archive with hopes of emerging with a short historical side project describing a case known among geeks as "Scientology vs. the Internet." Being more accustomed to interviewing people than making sense of heaps of (in this case, very strange) documents, Kent thankfully and graciously walked me through the confusing, fascinating, and at times disturbing innards of an organization so many geeks love to loathe.

In January 2008, my historical project leaped into the present when, in the course of targeting the Church of Scientology, Anonymous underwent a broader and surprising metamorphosis from fearsome pranksters to fervent protesters. I was hooked. It seemed only natural to follow these mad hatters and see if anything would come of their bold and unexpected foray into protest culture—and clearly something did. By that time I had relocated to New York City and discovered a physical portal into Anonymous through the rambunctious local cell that welcomed me to its monthly protests. In turn, I welcomed members of the cell into my classroom, where my students and I benefited from both their eloquent lectures on the political significance of Anonymous and their theatrical antics demonstrating the lulz. Little Sister, Sethdood, and Matthew "PokeAnon" Danziger met with me on numerous occasions and proved lively interlocutors. The latter two even sat for formal interviews. I also experienced the delight of close acquaintance with Chanology Dublin and other Irish Anons; they were some of my most intrepid teachers. I crossed the ocean to draw upon this valuable resource on numerous occasions, and by my third trip in a three-year span, it was clear that a few of them, notably Pete, David, Firefly, and Donncha, had become more than sources—they had become friends. I look forward to future exchanges.

In 2010, when Anonymous broke into public consciousness with its direct-action digital campaign protesting the banking blockade leveled against WikiLeaks, I was fortuitously on sabbatical at a sanctuary—the Institute for Advanced Study at Princeton. The punishing pace of activity that subsequently cascaded from the AnonOps network would have been nearly impossible to follow were it not for the glut of time I was afforded. Conversations with two colleagues in my cohort, Manu Goswami and Tanya Erzen, helped shape my thinking on the topic. Anthropologist Didier Fassin proved an inspirational mentor, whose boundless willingness to share feedback was confirmed again after I presented on Anonymous at a recent workshop on public ethnography held at the IAS.

As 2010 turned into 2011, I lost myself full time in the ever-shifting maze of Anonymous. At times ambling with no direction or purpose, and at other times ardently driven to fulfill a mission, I spoke with dozens upon dozens of participants, benefiting from their time, experiences, insights, and critiques. I thank every one of you and I am sorry for my inability to remember and list all of your names—whether real, fake, or pseudonymous. A few folks necessitate special mention, going beyond the call of duty in their willingness to guide me. Early on, Trivette, meddle, and n0pants each spoke to me one-on-one and opened various doors in so doing. I found welcome homes in #reporter, #freedommods, and eventually #cabincr3w, where conversations ran into the hours and were always lively and illuminating. Over time, a handful of other folks put me on different paths of thinking. Anonymous9—teeming with energy—was inexhaustibly helpful. This book, at least in this form, would simply not be possible without him. m0rpeth was probably the first of a handful of insiders to implore me to stop drinking the Kool-Aid; his trenchant critiques of emergent power structures made it easier for me to intuit them and, in so doing, apprehend the many strains of internal critique existent in Anonymous. blackplans, a

consistent presence spanning different eras and scenes, was boundlessly erudite and witty about Anonymous and hackers (not to mention life in general). Andrew Auernheimer, certainly far from being anonymous, or a fan of Anonymous, taught me a lot about trolling, often through his trollish arguments and statements, but thankfully never trolled me. Many others spent quite a bit of time chatting with me, including c0s, AnonyOps, Barrett Brown, evilworks, q, mr_a, sharpie, Katanon, shitstorm, owen, Avunit, emmi, Jackal, p0ke, crypt0anonymous, Nicole Powers, Nixie, Commander X, JMC, papersplx, Lauri Love, and others who will remain anonymous.

Over time (and due to a string of arrests), the circumstances of my research changed in equal measure with the public perception of its subjects. Many Anons have endured difficult legal battles and time in prison. Given just how complicated their lives became, I am all the more grateful that they made time for me. The book could simply not have been completed without the generosity and the acumen of Jeremy Hammond, Mustafa Al-Bassam, Donncha O'Cearbhaill, Darren Martyn, and Mercedes Haefer, each of whom poured hours into answering endless strings of sometimes repetitive questions. Chris Weatherhead and Jake Davis also met with me in person to share many of their experiences; Ryan Ackroyd, who I only started to interact with recently, commented thoughtfully on the "Internet Hate Machine" and informants.

During research I could be found chatting with a number of journalists and filmmakers who, like me, spent an enormous about of time toiling away trying to crack the Anonymous puzzle. Their presence was welcome—talking shop and trading some research notes proved to be both comically relieving and professionally invaluable. Conversations with Quinn Norton, Asher Wolf, Steve Ragan, and Brian Knappenberger were instrumental to my thinking on Anonymous. Steve Ragan also deserves special mention for sharing so freely—most journalists are far more guarded about their possessions. Knappenberger's film and Parmy Olson's engrossing account

of Anonymous and LulzSec proved to be valuable resources for this project.

In 2013, a slew of colleagues read a couple of early chapters and dispensed thoughtful commentary: Danielle Citron, Nathan Schneider, Jonathan Sterne, Darin Barney, Christine Ross, Carrie Rentschler, Sandra Hyde, Michael Ralph, Whitney Phillips, and Chris Kelty. Over the years, I have lectured extensively on Anonymous, and it would be impossible to take stock of all the bountiful feedback I received; however, comments from Paul Eiss, Angela Zito, Faye Ginsburg, Haidy Geismar, Daniel Miller, Alberto Sanchez, and Bob Rutledge are of particular note.

At McGill University, I am fortunate to hold a position designed to enable my engagement in both outreach and writing; I am deeply grateful to the generous donor who provides its funding. The environment at McGill has proved stimulating, and I am especially thankful to all the Bits, Bots and Bytes participants for contributing to a research forum and scholarly exchange that has become one of the highlights of my month. Two of its members, Scott Kushner and Elena Razlogova, read and commented incisively on additional material shared outside of the meet-up. My undergraduate student and unflagging research assistant Maya Richmond has successfully hunted down every last bit of material I asked her to procure while also providing sharp insights regarding hackers and tricksters. Caroline Habluetzel, who received a PhD from our department, also provided invaluable and meticulous research assistance, all while battling cancer. She passed away in May 2013 and will be missed. My graduate class, "Technological Underworlds," was given an early draft of the first five chapters to read, resulting in fascinating questions and the identification of various problems. Darcie DeAngelo went beyond the call of duty to provide extensive commentary. Molly Sauter was completing her own book—*The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet*—throughout the same period,

and reading the manuscript proved both essential and fascinating as I worked through the ethics of digital direct action.

Writing a book for a popular audience while remaining faithful to complex, esoteric, technical, and legal details is a formidable challenge. I sought the advice of a host of experts to ensure that I was not misrepresenting these nuances. Orin Kerr, Marcia Hoffman, Ahmed Ghappour, and Andres Guadamuz read through the legal sections. Many technologists and hackers always delivered answers to my many questions: David Mirza, Chris Soghoian, Dino A. Dai Zovi, Chris Wysopal, Space Rouge, James Atkinson, Patrick Gray, Dan Guido, Morgan Marquis-Boire, and Brian Martin. Meanwhile, journalists Kim Zetter and Ted Bridis clarified some uncertainties I held about hackers and FBI policies toward informants. Any inaccuracies that remain stem from my inability to follow the excellent guidance of these consultants.

Family members should be thanked for enduring the negative consequences of book writing—and the Andersons were patient and gracious as the last three holiday seasons saw me not quite as present as everyone else. My father, an unflagging supporter of my work, ensured that his friends, most of them retired, learned something important about Anonymous. My dog Roscoe, with his cute snaggletooth, was daily able to woo me from my desk, ensuring that I took necessary breaks from writing.

Finally, there are three people whose imprint is everywhere in this book and who have read it start to finish, two of them more than once. My partner Micah Anderson, who spends his days (and too often nights) running a privacy-friendly ISP, is a talented writer. He read the first few chapters, took me aside, and clued me in to the fact that I needed to be far more lively and descriptive if this was to be a nonacademic/popular book. His subsequent readings of every chapter always generated useful comments or edits. He certainly doused with gasoline all my attempts at humor, before throwing a match and fueling the fire with jokes of his own. Some were just

too wild and imaginative and I had to stamp the fire out, but in the aftermath, things were typically much improved. I am extremely thankful that he is willing to be part of the creative process, and that he put up with me as I wrote two books back to back—something I will never, ever do again.

In part because of Micah's advice—and in part due to my own proclivity to explain everything—I went completely overboard with writing. Two people were poised to contain me, call out my inconsistencies, help me whittle the manuscript down to an appropriate size, and generally do everything in their power to make this a better book.

First, my research assistant Matt Goerzen, who is also my MA student and a quirky and talented artist specializing in, among other topics, anonymity, was a first line editor. Trained as a journalist, he is also a dexterous writer gifted in adding a touch of grace and clarity to any prose that comes his way. Since he has deeply pondered and completed so much research on the cultures of online anonymity, his comments were sharp and discerning. This book is much stronger because of his unstinting willingness to impart his wisdom. I will be forever grateful that he took on the role of my most trusted guide and interlocutor, and I only hope I can return the debt as his MA thesis supervisor.

When entertaining possible publishers, I wanted one that would help me reach the right balance between analysis and accessibility; Verso immediately presented itself as the number-one candidate and it has been a pleasure working with the entire team, including Mark Martin, Colin Beckett, Jennifer Tighe, and Jacob Stevens. I am especially grateful to have worked with Andrew Hsiao. When my book ballooned to an unacceptable size, I will confess that I dreaded the stringent measures he might enact to trim the manuscript. As I feared the worst, his advice ultimately proved both stellar and specific, making the pruning process far less painful than could have been. He went through the manuscript with a fine-tooth comb; he was persnickety about the small details of phrasing, he entertained

the value of my arguments, and he zoomed out to identify the sections, sentences, and even chapters where shaving and cutting were necessary. There were moments when, if it were possible to hug someone through email, I would have hugged him, multiple times. I have also thoroughly enjoyed our conversations about publishing and politics and look forward to many more in the future.

Finally, I would like to thank all of the masked activists and pranksters for staging this wildly epic play and giving me the opportunity to write about it.

A Note on Sources

In presenting a popular ethnography of Anonymous, this book leans heavily on journalistic convention and sourcing methodologies. Many readers will wonder how the information contained herein can be verified, given that lies, guile, and fabrication are the tools of the trade—often wielded with pride—by those operating under the mantle of Anonymous. But while some of the anecdotes recorded remain unverifiable, or simply accompanied by chat logs, they complement a factual narrative largely made possible by legal records. Indeed, this book could not have been written were it not for the unmasking of many participants upon their arrest and prosecution—and the troves of careful (and sometimes problematic) information made public by law enforcement toward this end. Additionally, while anonymity by nature enables individuals to speak out against and challenge powerful institutions, upon capture and sentencing many participants are suddenly afforded a different sort of freedom: the ability to speak honestly about their personal identities and experiences as individuals, distanced from a collective or protective pseudonym. Access to chat logs and especially court documents has further enabled me to authenticate many claims made by Anons and their colleagues prior to arrest (in the great majority of instances what I had been told turned out to be true).

The extensive chat logs cited in the book come from numerous sources: from public IRC channels, from published logs put online by Anonymous, from private logs given to me, and finally from logs submitted as court evidence and leaked to reporters. In instances where no documents existed, I have attempted to interview multiple participants and relied, where possible, on accounts published by respected media figures. It is a sad reality that many fascinating tales and participants, unable to be substantiated beyond rumor, were not included in these pages. Since many of the figures covered in this book are now well known to the public—and have been written about extensively—I have not changed their names or their pseudonyms, except in instances where not doing so might pose a threat to the individual in question.

This book should be read as a collection of personal experiences and reflections. While I address major events and historical turning points, and attempt to be inclusive of multiple (even, at times, conflicting) perspectives, there is much more at work within Anonymous than what is in these pages.

Epilogue: The State of Anonymous

1. Frank Bajak, "Top South American Hackers Rattle Peru's Cabinet," bigstory.ap.org, Sept. 2, 2014.
2. See the Gamma Group homepage at https://www.gammagroup.com/, last accessed July 21, 2015.
3. WikiLeaks, "The Spy Files: GAMMA FINFISHER TROJAN," wikileaks.org, last accessed July 21, 2015, available at https://wikileaks.org/spyfiles/list/tags/gamma-finfisher-trojan.html.
4. Morgan Marquis-Boire and Bill Marczak, *From Bahrain With Love: FinFisher's Spy Kit Exposed?*, The Citizen Lab, July 25, 2012, available at https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/. Though the researchers could not confirm it was the government who sent the software, it was suspicious that the captured data was sent to a Bahrain IP address. For Gamma's denial, see Vernon Silver, "Gamma Says No Spyware Sold to Bahrain; May Be Stolen Copy," bloomberg.com, July 27, 2012.
5. Cora Currier and Morgan Marquis-Boire, "Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters," firstlook.org/theintercept, Aug. 7, 2014.
6. "Hack Back", n.d., last accessed July 21, 2015, available at http://0x27.me/HackBack/0x00.txt.
7. Ibid.
8. Cora Currier and Morgan Marquis-Boire, "Leaked Documents Show FBI, DEA and US Army Buying Italian Spyware," firstlook.org/theintercept, July 6, 2015.
9. Hacked Team, Twitter post, July 5, 2015, 5:26 pm, available at, http://core0.staticworld.net/images/article/2015/07/hackingteam_1-100594937-orig.jpg, last accessed July 21, 2015.
10. Phineas Fisher, Twitter post, July 5, 2015, 11:04 pm, https://twitter.com/GammaGroupPR/status/617937092497178624.
11. Anon2World, Twitter post, June 25, 2015, 8:48 pm, https://twitter.com/Anon2earth/status/614279036278284288.
12. Steven Chase, "Cyberattack Deals Crippling Blow to Canadian Government Websites," theglobeandmail.com, June 17, 2015.
13. See reporter's transcript of proceedings held on Thursday, January 22, 2015, available at https://pdf.yt/d/0SWY7AoPOoovRD_a, last accessed July 21, 2015.
14. Ibid.
15. Quinn Norton, "We Should All Step Back from Security Journalism," medium.com, Jan. 23, 2015.
16. Available at http://freelauri.com/, last accessed July 21, 2015.
17. Tor, "Interview with Tor Summer of Privacy Student Donncha O'Cearbhaill," last accessed July 21, 2015, available at https://

blog.torproject.org/blog/interview-tor-summer-privacy-student-donncha-ocearbhaill.

18. See for example Lee Rainie and Mary Madden, *Americans' Privacy Strategies Post-Snowden,* Pew Research Center, March 16, 2015, available at http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.
19. James B. Comey, "Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?," speech given at Brookings Institution, October 16, 2014, last accessed July 21, 2015, available at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.
20. Helen Nissenbaum, "The Meaning of Anonymity in an Information Age," *Information Society*, vol. 15, no. 2 (May 1999): 141–4.
21. Available at https://thepaypal14.com/story-keth.htm, last accessed July 21, 2015.
22. See https://twitter.com/ro0ted, last accessed July 23, 2015.
23. See correction provided at the end of Matthew Braga, "Anonymous Claims It Leaked Passwords and Credit Card Info of Canadian Officials," motherboard.vice.com, June 23, 2015.
24. Peter Sterne, "Gawker in the Fight of Its Life with Hulk Hogan Sex-Tape Suit," capitalnewyork.com, June 12, 2015.
25. Editors, "N*ewsweek*'s Statement on the Bitcoin Story," newsweek.com, March 7, 2014.
26. While it does not appear he has moved forward with a lawsuit, some Bitcoin enthusiasts hosted a crowdsourced fundraising campaign to help support Nakamoto and raised the equivalent of approximately $14,000USD in Bitcoin. See "Dorian Nakamoto—Thank You, Bitcoin Community," YouTube video, posted by aantonop, April 22, 2014, last accessed July 23, 2015, available at https://www.youtube.com/watch?v=w7YmJZ-qVW8.
27. Julian Assange, "Assange: How 'The Guardian' Milked Edward Snowden's Story," newsweek.com, April 20, 2015.
28. Siobhan Gorman, "Alert on Hacker Power Play," wsj.com, Feb. 21, 2012.
29. For the Twitter tirade see this thread. Anonymous, Twitter post, Aug. 14, 2014, 8:14 am, https://twitter.com/Crypt0nymous/status/499937201825001472.
30. Jack Bratich, "Popular Secrecy and Occultural Studies," *Cultural Studies*, vol. 21, no. 1 (January 2007): 42–58.
31. See also Clare Birchall, "Transparency, Interrupted: Secrets of the Left," *Theory, Culture and Society,* vol. 28, no. 7/8 (December 2011): 60–84.
32. For an anthropological analysis of the insidious contemporary logics of American state secrecy, see Joesph Masco, *The Theater of Operations: National Security Affect from the Cold War to the War on Terror* (Durham, NC: Duke University Press, 2014).

33. Julian Assange, et al., *Cypherpunks: Freedom and the Future of the Internet* (New York: OR Books, 2012), 5.
34. See especially Darin Barney, "Publics without Politics: Surplus Publicity as Depoliticization," in *Publicity and the Canadian State: Critical Communications Perspectives,* ed. Kirsten Kozolanka (Toronto: University of Toronto Press, 2014), 70–86.
35. Robin Celikates, "Civil Disobedience as a Practice of Civic Freedom," in *On Global Citizenship: James Tully in Dialogue,* series ed. David Owen (New York: Bloomsbury, 2014), 223.
36. Ewen MacAskill, "Second Leaker in US Intelligence, Says Glenn Greenwald," theguardian.com, Oct. 11, 2014.
37. See Fruzsina Eördögh, "How Big Is Anonymous? Maybe Bigger than You Thought," csmonitor.com, July 8, 2015, for an article covering a recent sociological study on Anonymous' presence on Facebook that suggests the protest ensemble is both larger and more global than previously assumed.
38. Personal interview, June 15, 2015.
39. See Celia Britton, "Opacity and Transparency: Conceptions of History and Cultural Difference in the Work of Michel Butor and Edouard Glissant," *French Studies*, vol. 49, no. 3 (July 1995): 308–20.