

# Electronic Communications Surveillance

LAUREN REGAN

*“I think you’re misunderstanding the perceived problem here, Mr. President. No one is saying you broke any laws. We’re just saying it’s a little bit weird that you didn’t have to.”*—John Oliver on *The Daily Show*<sup>1</sup>

The government is collecting information on millions of citizens. Phone, Internet, and email habits, credit card and bank records—virtually all information that is communicated electronically is subject to the watchful eye of the state. The government is even building a nifty, 1.5 million square foot facility in Utah to house all of this data.<sup>2</sup> With the recent exposure of the NSA’s PRISM program by whistleblower Edward Snowden, many people—especially activists—are wondering: How much privacy do we actually have? Well, as far as electronic privacy, the short answer is: None. None at all. There are a few ways to protect yourself, but ultimately, nothing in electronic communications is absolutely protected.

In the United States, surveillance of electronic communications is governed primarily by the Electronic Communications Privacy Act of 1986 (ECPA), which is an extension of the 1968 Federal Wiretap act (also called “Title III”) and the Foreign Intelligence Surveillance Act (FISA). Other legislation, such as the USA PATRIOT Act and the Communications Assistance for Law Enforcement Act (CALEA), supplement both the ECPA and FISA.

The ECPA is divided into three broad areas: wiretaps and “electronic eavesdropping,” stored messages, and pen registers and trap-and-trace devices. Each degree of surveillance requires a particular burden that the government must meet in order to engage in the surveillance. The highest burden is in regards to wiretaps.

---

**LAUREN REGAN** is the executive director and staff attorney of the Civil Liberties Defense Center in Eugene, Oregon. This information is constantly changing; to keep yourself updated, consider becoming a member of the Civil Liberties Defense Center and receive our weekly action alerts and updates (<http://cldc.org>). The information contained in this article is not intended as legal advice nor does it form an attorney-client relationship. Thanks to Cooper Brinson at the University of Oregon for research assistance on this article.

## Wiretapping and Electronic Eavesdropping

Under ECPA, it is unlawful for any person to intercept or attempt to intercept wire, oral, or electronic communications by means of an electronic, mechanical, or any other device unless such conduct is authorized or not covered.<sup>3</sup> Wiretaps are unique in that they capture the content of communications, i.e., they reveal the purpose and meaning of a particular communication, not just the outlying “metadata.”<sup>4</sup> Interestingly, silent video surveillance is not prohibited under this particular statute.

Prior to the adoption of ECPA or FISA, in 1967 the U.S. Supreme Court in *Katz v. United States*, formed a baseline test to determine whether the monitoring of certain communications violated the Fourth Amendment.<sup>5</sup> The test is centered on whether the individual being monitored can *reasonably expect* the communications at issue to be, in fact, private. In his concurrence, Justice Harlan summarizes the test: “there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable.”<sup>6</sup> This standard is currently the measure in deciding whether a wiretap violates the ECPA.

Some entities and situations are exempt from the prohibition on wiretapping.<sup>7</sup> For instance, businesses conducting wiretapping as a part of their ordinary business practices may be permitted to monitor communications provided that such monitoring is routinely performed and done for a “legitimate business reason.” In many jurisdictions, businesses are required to notify their employees of monitoring. Jails, prisons, and other law enforcement institutions regularly record phone and other electronic communications.<sup>8</sup>

## CALEA, FISA, and Wiretapping

Perhaps the most significant legal development in regards to wiretapping came in 1994 with the passing of the Communications Assistance for Law Enforcement Act (CALEA).<sup>9</sup> Under CALEA, telecommunications providers and manufacturers have a general “duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes.”<sup>10</sup> Specifically, however, CALEA requires that telecommunications providers “ensure that...equipment, facilities, or services” are built in such a way as to allow federal agencies the power to monitor communications sent through such equipment, facilities, or services.<sup>11</sup> Currently, CALEA extends to telephone, Internet, and Voice over Internet Protocol (VoIP) communications.<sup>12</sup> Interestingly, telecommunications providers are not responsible for decrypting messages that have been encrypted by customers.<sup>13</sup>

As a result of the exposure of extensive domestic warrantless surveillance, and as a result of the desire of the National Security Apparatus for some form of legislative and judicial approval of the warrantless “foreign intelligence” surveillance they had long conducted, in 1978 Congress passed FISA.<sup>14</sup> The stated intent of FISA was to limit surveillance of U.S. citizens—restricting invasive surveillance techniques to collecting information on “foreign powers” and “agents of foreign powers.” Nevertheless, FISA allows the president to “authorize electronic surveillance without a court order...for periods of up to one year.”<sup>15</sup> In order for the president’s request to be granted, the attorney general must certify, in writing and under oath, that a number of conditions are satisfied. This certification is then submitted to—not reviewed by—the Foreign Intelligence Surveillance Court (FISC) and the Senate Select Committee on Intelligence. In other words, the president may authorize warrantless searches so long as the attorney general swears that the searches comply with FISA. Other federal police agencies must submit a request to FISC. The request is then denied or approved by a panel of three judges. The only catch is that this court is secret—its opinions are not subject to public scrutiny, and documents that are made public are heavily redacted. Between 1979 and 2012, federal police agencies submitted 33,942 FISA surveillance requests. Only eleven requests were denied.<sup>16</sup>

Under the Patriot Act, the powers granted to the executive branch were substantially broadened. One of the most significant changes involves the entire stated purpose of FISA. Prior to the Patriot Act, FISA required that agents seeking authorization to spy declare, “the purpose...of the surveillance is to obtain foreign intelligence information.” After the Patriot Act, the statute now requires that agents only assert, “that a *significant* purpose of the surveillance is to obtain foreign intelligence information” (emphasis added).<sup>17</sup> The change in language significantly broadens the circumstances in which surveillance may be authorized. The domestic U.S. result of this change was to void the limited protection offered by the preexisting rule that once the purpose of the warrantless foreign intelligence surveillance shifted to criminal prosecution, the fruits of ongoing “foreign intelligence” warrantless surveillance could no longer be used in court.<sup>18</sup>

Additionally, the Patriot Act amended 50 U.S.C. § 1805(c)(2)(B), to authorize what is known as a “roving wiretap.”<sup>19</sup> Essentially, a roving wiretap “allows the interception of any communications made to or by an intelligence target without specifying the particular telephone line, computer or other facility to be monitored.”<sup>20</sup> According to EPIC, “prior

law required third parties (such as common carriers and others) ‘specified in court-ordered surveillance’ to provide assistance necessary to accomplish the surveillance—under the new law, that obligation has been extended to unnamed and unspecified third parties.”<sup>21</sup>

A number of challenges have been made to the U.S. government’s domestic spy programs. However, most of the significant challenges have been tossed out on procedural grounds. With the recent revelations surrounding PRISM, what the next round of litigation offers remains to be seen.<sup>22</sup>

### **How Does the Government Actually Spy? Inherent Vulnerabilities in Electronic Communications**

#### **E-mail**

Email is extraordinarily vulnerable. Messages “travel” through a number of different channels before their arrival with the intended recipient. At any one of these channels, an email can be intercepted and its content viewed. If your email is not encrypted, the content of your messages is at its most vulnerable in terms of being viewed by a third party.<sup>23</sup>

Email messages can be intercepted and then reformatted to be sent to the intended recipient or someone else altogether. This kind of interception is called a “man-in-the-middle-attack.”<sup>24</sup> Email addresses can be disguised as another person or organization in a process called masquerading.<sup>25</sup> A more invasive and insidious form of disguise is spoofing, in which email addresses are actually forged.<sup>26</sup> Thus, Suzy may think she is getting an email from her longtime friend, Bill, but in fact, it is from an unknown third party. It’s not just private security firms or government agencies that have access to spoofing—everyday Internet users can disguise themselves with the help of websites like Fogmo.com. Emails can also be disabled through Denial of Service Attacks (DoS) or Distributed Denial of Service Attacks.<sup>27</sup> These attacks can be carried out through a variety of methods, and there is little protection against them.

#### **Mobile Phones**

Cell phones, through either triangulation or multilateration, constantly track your location.<sup>28</sup> However, many of these processes are irrelevant since many smartphones now have built in GPS that is recorded and stored.

Government agencies are typically required to get a court order before monitoring cell phone use (via a pen register and/or trap and trace device) but with the recent exposure of programs like PRISM, it’s clear that this requirement is often ignored.<sup>29</sup> These court orders are

used almost exclusively for the purpose of compelling a communications service provider to turn over records and information needed to track a cell phone user. But, with technology like “triggerfish,” federal police agencies, at least at a technical level, do not have to go through the communications company—that is, the court order would simply be a courteous formality in terms of actually getting the desired information to track a person.<sup>30</sup> Triggerfish is a technology that mimics a cell phone tower, picking up on a cell phone’s signal and essentially, through a man-in-the-middle attack, intercepts calls and reveals numbers dialed and received, locations, and other information that can pinpoint the identity of the cell phone user. In fact, some suspect that triggerfish was used to round-up the RNC [Republican National Convention]-8 in 2008.<sup>31</sup> The technology known as “Stingray” is essentially the same as triggerfish.<sup>32</sup> A similar technology called an IMSI-catcher can also be used to intercept cell phone calls and data, though its utility is limited compared to triggerfish or stingray. Tools are available in order to protect yourself when using a mobile phone.<sup>33</sup> Note, however, that like most forms of electronic communication, there is no absolute protection against surveillance. You can make it extraordinarily difficult for people or technologies to gather your data, but no protection is absolutely impassable.

### **Intelligence Programs and Methods**

Law enforcement agencies are involved in a number of multi-agency operations to spy on individuals and groups, both domestic and foreign. These include:

**Boundless Informant** is a computer system used by the NSA to compile and make sense of data collected in various data mining schemes. The system does not compile FISA data.<sup>34</sup>

**X-KEYSCORE** is a program developed and used by the NSA that provides the “widest-reaching” access to information about individuals’ online activity. The program allows its user to view emails, chats, browsing histories, and “nearly everything a typical user does on the internet.” Analysts using the program can access information with no prior authorization from courts or even a signature from a supervisor. The analyst simply fills out an online form with a brief “justification” and a time-frame for the particular data sought. Screen-shots and the NSA’s presentation illustrate the format of the system. The plug-ins used by analysts operating with X-KEYSCORE are the reason we can say: there is no online privacy. These plug-ins can uncover VPN (Virtual Private Network, used to create a secure session between a user and a

private network) and PGP (Pretty Good Privacy, (a widely used open source data encryption standard for email and files) users. And aside from these tools, I know of nothing that can make a considerable difference with respect to the protection of peoples's electronic privacy.<sup>35</sup>

DCSNet (Digital Connection Systems Network) is a surveillance system used by the FBI to wiretap cell phones (including SMS text messaging) and landlines.<sup>36</sup> The system allows agents to easily access wiretapping posts located throughout the country through a "point-and-click" interface.<sup>37</sup> DCSNet is run on a secure "Peerless IP fiber network" developed and maintained by Sprint.<sup>38</sup> The network is not connected to the public internet. DCSNet was built from the remnants of Carnivore—a spy software tool utilized by the FBI.<sup>39</sup>

NSA Call Database contains the records of "billions" of call records of U.S. citizens. The call records are from AT&T and Verizon. Most of the records collected are from citizens who are not suspected of any crime. The database is apparently the largest of its kind in the world.<sup>40</sup>

**AT&T and the NSA.** According to the Electronic Frontier Foundation (EFF):

AT&T's internet traffic in San Francisco runs through fiber-optic cables at an AT&T facility located at 611 Folsom Street in San Francisco. Using a device called a 'splitter,' a complete copy of the internet traffic that AT&T receives—email, web browsing requests, and other electronic communications sent to or from the customers of AT&T's WorldNet Internet service from people who use another internet service provider—is diverted onto a separate fiber-optic cable which is connected to a room, known as the SG-3 room, which is controlled by the NSA. The other copy of the traffic continues onto the internet to its destination.<sup>41</sup>

The exposure of this program culminated in a lawsuit, *Hepting v. AT&T*, in which EFF sued AT&T and Verizon for "violating privacy law by collaborating with the NSA in the massive, illegal program to wiretap and data-mine American's communications." After surviving the government's motion to dismiss, the case was appealed to the Ninth Circuit and then was dismissed. The court held that AT&T and Verizon have retroactive immunity from suit under amendments made to FISA in the FISA Amendments Act of 2008.<sup>42</sup>

TALON ("Threat and Local Observation Notice") was a U.S. Air Force database that stored information on individuals and groups who allegedly pose threats to the United States.<sup>43</sup> After the database was exposed for having collected mass amounts of information on peace groups and activists, the government announced that it would shut the database down and transfer data to the FBI's Guardian database.

**Guardian** (“Guardian Threat Tracking System”) is, according to the FBI, an “automated system that records, stores, and assigns responsibility for follow-up on counterterrorism threats and suspicious incidents. It also records the outcome of the FBI’s handling of terrorist threats and suspicious incidents.” To give an idea of the breadth of this system, a 2007 internal audit of the system found that between July 2004 and November 2007, 108,000 “potential terrorism-related threats, reports of suspicious incidents, and terrorist watchlist encounters” were recorded. The audit notes that “the overwhelming majority of the threat information documented in Guardian had no nexus to terrorism.”<sup>44</sup>

**ADVISE** (“Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement”) was a massive database/computer system used by Homeland Security that captured and analyzed personal data of U.S. citizens. The project was essentially a data-mining operation.<sup>45</sup>

**Magic Lantern** is a software program developed by the FBI that logs keystrokes, i.e., records what is typed. There are a number of different types of “keyloggers.”<sup>46</sup> Essentially, keystroke software like Magic Lantern bypasses the protection typically offered by encryption. Magic Lantern can be installed through an email with an attachment (a trojan horse) or through other nefarious means.<sup>47</sup> Keyloggers are typically unknown to the user being logged.

### Protecting Yourself

Here is the bottom line: *You don’t really have any privacy when it comes to electronic communication. There are no absolute protections in electronic communication. Your cell phone, email, social media, and any other form of communication are subject to surveillance.* However, in light of PRISM and the extent of NSA surveillance, the *Washington Post* has suggested a few ways to protect yourself against the NSA (note, these are *in no way* absolute protections):<sup>48</sup>

- Browse the Internet with Tor or through a “virtual private network.”<sup>49</sup>
- Use OTR to encrypt chats.<sup>50</sup>
- Use “Silent Circle” or “Redphone” to make phone calls.<sup>51</sup>
- Take out your phone battery.<sup>52</sup>

Additionally, and directly relevant to activists, Riseup has offered a number of services to protect against online surveillance.<sup>53</sup>

### Grey Intelligence and Government Collusion: Attacks upon Dissent

One of the common threats to all movements, activists, and global citizens is the attack upon the rights to privacy, organizing, and dissent



that is being wrought by the government-corporate surveillance state. Anyone who has heard the news lately should be fairly acquainted with the outrageous surveillance conducted by the NSA and several other agencies against every phone call or Facebook post you have ever made. Many might be surprised to hear that the military infiltrated and spied on peace activists in Washington.<sup>54</sup> Or that the FBI has been recruiting young women from college classrooms to spy upon, and entrap young anarchist/environmental activists while pretending to date the male victims.<sup>55</sup> And even more disturbing, the U.S. government has colluded with private corporations and extractive industries to ratchet up their COINTELPRO-esque tactics upon climate justice activists. The few constitutional protections that exist to limit the ability of the feds to spy on political organizations and activities are exploited by their partners in the “grey intelligence” realm of corporate spying.


Some 1,271 government organizations and 1,931 private companies work on programs related to counterterrorism, homeland security, and intelligence in about 10,000 locations across the United States.<sup>56</sup> “By 2007, 70 percent of the U.S. intelligence budget—or about \$38 billion annually—was spent on private contractors.” One defense analyst says that today, overall annual spending on corporate security and intelligence is roughly \$100 billion, double what it was a decade ago.<sup>57</sup>

To give you an example of how this is playing out: a climate justice group—whether fighting fracking, coal, tar sands or pipelines—engages in completely lawful, constitutionally protected First Amendment activity, like holding a banner on a street corner. Big industry creates a side business that includes “private security” and “public relations” components in order to keep their hands clean. The private spies are often former FBI head honchos who leave government service for the lucrative land of corporate paychecks, but remain well-connected to their former employers and coworkers. Private spies infiltrate the group, create problems, steal membership or financial information from the group, and sometimes hack computers and/or attempt to provoke the group to break the law (or escalate tactics without group consent). Then they bring the information back to the PR staff, who grossly and maliciously manipulate facts and create a written publication called a “Terrorist Bulletin,” which is produced and sent to fellow industry organizations, as well as federal and local law enforcement. These terrorist bulletins say things like, “This group is lawful and nonviolent now, but they are getting more militant and may become violent in the near future.” In addition, these grey intelligence organizations come up with strategies to destroy and discredit lawful political groups.<sup>58</sup>



Case in point: the U.S. Chamber of Commerce hired a law firm, who in turn, hired a consortium of private intelligence firms in order to discredit their perceived opponents in U.S. Chamber Watch, which included watchdog organizations and labor unions. As a result of a memo leaked by Anonymous (a hacktivist group), evidence of their defamatory COINTELPRO hijinks were clearly uncovered. In the “Information Operations Recommendation,” the authors state they “need to discredit the organization through the following:” snitch-jacketing the leaders, planting false information and spies within the group, and using mainstream media to embarrass and derogate the organization. They admit, “unlike some groups, members of this organization are politically connected and well established, making the US Chamber Watch vulnerable to information operations that could embarrass the organization and those associated with it” (see below).<sup>59</sup>

In addition, it has become commonplace for corporations like TransCanada to provide PowerPoint presentations to local and federal




---

Information Operations Recommendation

Subject: US Chamber Watch Information Operations Recommendation

Date: November 29, 2010

Summary

US Chamber Watch is one of the most active members of the opposition to the US Chamber of Commerce (CoC). Unlike some groups, members of this organization are politically connected and well established, making the US Chamber Watch vulnerable to information operations that could embarrass the organization and those associated with it.

Details

US Chamber Watch is well connected politically, evidenced by the established relationship between CtW and Andy Stern, and is associated with many powerful DC operatives behind the scenes. The organization typically does not use theatrical performances or overt gestures. The people in this case are less important than the organization. Therefore we need to discredit the organization through the following.

1. Paint US Chamber Watch as an operative of CtW and the unions, while at the same time highlighting the organization of the unions against the chamber. We should show also the flow of members from unions to CtW as well as the closeness of CtW and US Chamber Watch.
2. Craft a message to combat the messaging propaganda of US Chamber Watch. For example, target how the unions are being an inhibitor to progress by advocating for unrealistic individual benefits, while the Chamber continues its focus on job creation through innovation in order to showcase how the US economy prospers in the global economy. Packaged in the right mediums, such an operation can prove to be powerful.
3. Create a false document, perhaps highlighting periodical financial information, and monitor to see if US Chamber Watch acquires it. Afterward, present explicit evidence proving that such transactions never occurred. Also, create a fake insider persona and generate communications with CtW. Afterward, release the actual documents at a specified time and explain the activity as a CtW contrived operation. Both instances will prove that US Chamber Watch cannot be trusted with information and/or tell the truth.
4. Connect US Chamber Watch's radical tactics to Velvet Revolution, explaining that both entities are loosely operating together. Depending on the level of connection established, such an approach may need to be spotlighted as more of a conspiracy rather than a separate, vocal persona.
5. If needed, create two fake insider personas, using one as leverage to discredit the other while confirming the legitimacy of the second. Such work is complicated, but a well-thought out approach will give way to a variety of strategies that can sufficiently aid the formation of vetting questions US Chamber Watch will likely ask.
6. Create a humor piece about the leaders of CtW.

law enforcement, as well as District Attorneys and other prosecutors, where the tar sands industrial giant provides them with information on political organizers and advocates terrorism investigations and prosecutions of nonviolent activists engaged in political campaigns against the irreparable destruction of the planet.<sup>60</sup> I provide legal support to the Tar Sand Blockade, a Texas-based nonviolent frontlines direct action group resisting the southern portion of the TransCanada KXL pipeline.<sup>61</sup> At one lawful protest that I witnessed, local rural residents lined the side of the road holding signs in opposition to the pipeline, while other activists perched in trees that were to be cut to make way for the pipeline route. Local untrained sheriff's deputies began indiscriminately pepper-spraying the crowd of bystanders that included elders and children. After the cop riot was over, I witnessed the TransCanada representative walk up to one of the sheriff's deputies, slap him on the back, thank him for a job well done, and then offer to bring by more pepper spray to replenish the department's supplies. This outrageous collusion is not an isolated incident.

In another case, the director of the Pennsylvania Department of Homeland Security, James Powers, mistakenly sent an email to an anti-drilling activist he believed was sympathetic to the industry, warning her not to post industry terrorist bulletins online. In his email Powers wrote: "We want to continue providing this support to the Marcellus Shale Formation natural gas stakeholders while not feeding those groups fomenting dissent against those same companies."

Despite the attempts by government and corporations to crush the grassroots climate justice movements flourishing around the world, the number of activists and actions against these industries continues to grow on a daily basis. Only by taking control away from these corporations and their beholden government cronies will this egregious surveillance activity be curtailed; and the only way that will happen is by fostering a powerful mass movement capable of reclaiming our civil liberties and the virtuous right to dissent.

## Notes

1. Cited in Mike Masnick, "Daily Show Takes On NSA Surveillance: It's A Little Weird That Feds Didn't Have To Break Any Laws To Spy On Everyone," June 11, 2013, <http://techdirt.com>.

2. Howard Berkes, "Amid Data Controversy, NSA Builds Its Biggest Data Farm," June 10, 2013, <http://npr.org>.

3. The ESCA is 18 U.S.C.2511. According to

18 U.S.C.2510(6), "Person' means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation."

4. "Metadata" includes data about data, i.e., data void of necessarily meaningful content. For example, the kind of data gathered by pen registers (discussed below) that reveals the source and destination of a

communication but not the actual content of a communication is a form of metadata.

5. 389 U.S. 347 (1967), <http://law.cornell.edu/sup>.

6. *Ibid*, 361.

7. There are roughly five categories of exemptions to the prohibition of wiretapping: consent of one or more party; publicly accessible radio communications;

government officials; communication service providers; and situations involving a parent and a minor child or spouses.

8. Telephone conversations between inmates and clergy, however, are not subject to recording/monitoring. *Mockaitis v. Harderodad*, 104 F.3d 1522, 1530 (9th Cir. 1997).
9. Electronic Frontier Foundation, "CALEA: The Perils of Wiretapping the Internet," <https://eff.org/issues/calea>.
10. 141 Cong. Rec. H113-05 (Oct. 25, 1994).
11. 47 U.S.C. § 1002.
12. For example, Skype or Google Talk.
13. "A telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication." 47 U.S.C. § 1002(b)(3). Interestingly, the feds (particularly the DEA) are having a very tough time decrypting Apple's built in encryption for text messages between iPhones. Dan Goodin, "Apple's iMessage Crypto Stymies Federal Eavesdropping of Drug Suspect," April 4, 2013, <http://arstechnica.com>.
14. "50 U.S. Code Chapter 36 - Foreign Intelligence Surveillance," <http://law.cornell.edu>.
15. 50 USCA § 1802.
16. "Foreign Intelligence Surveillance Act Court Orders 1979-2014," updated May 1, 2014, <http://epic.org>.
17. 50 USCA § 1804.
18. See *In re: Sealed Case No. 02-001*, 310 F.3d 717 (United States Foreign Intelligence Surveillance Court of Review 2002). The pre-existing rule was set out in *U.S. v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). It should be noted that the author of an article in this issue of *Monthly Review*, Michael E. Tigar, as well as the issue editor, John Mage, were trial and appellate counsel for Truong.
19. "Let the Sun Set on PATRIOT - Section 206: Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act of 1978," <http://w2.eff.org>.
20. "Foreign Intelligence Surveillance Act (FISA)," <http://epic.org>.
21. *Ibid.*
22. Charlie Savage, "A.C.L.U. Files Lawsuit Seeking to Stop the Collection of Domestic Phone Logs," *New York Times*, June 11, 2013, <http://nytimes.com>.
23. To learn encryption basics, see: "Message Security," <https://riseup.net/en/message-security>.
24. "Man-in-the-middle attack," <http://en.wikipedia.org>, accessed May 30, 2014. If you would like to know how to identify and defeat these kinds of attacks, see Christopher Soghoian and Sid Stamm, "Certified Lies: Detecting and Defeating Government Interception Attacks Against SSL," paper presented at Financial Cryptography and Data Security '11, Fifteenth International Conference, March 2011, <http://files.cloudprivacy.net/ssl-mitm.pdf>.
25. Symantec, "Configuring Email Aliases and Address Masquerades," August 20, 2012, <http://symantec.com>.
26. "Email Bombing and Spamming," <http://cert.org>.
27. "Denial-of-service attack," <https://en.wikipedia.org>.
28. eHow, "How to Triangulate a Cell Phone," <http://ehow.com>; "Multilateration," <http://en.wikipedia.org>.
29. "Pen register," accessed May 30, 2104, <http://en.wikipedia.org>; "The term 'trap and trace device' means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. §3127, <http://law.cornell.edu>.
30. Jonathan Racicot, "Cyber Espionage: The Triggerfish," November 19, 2008, <http://cyberwarfaremag.wordpress.com>.
31. Tom Burghardt, "Preemptive Policing & the National Security State: Repressing Dissent at the Republican Convention," November 18, 2008, <http://globalresearch.ca>.
32. Kim Zetter, "Feds' Use of Fake Cell Tower: Did it Constitute a Search?," November 3, 2011, <http://wired.com>; Zetter, "Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight," April 9, 2013, <http://wired.com>.
33. OsmocomBB, <http://bb.osmocom.org/trac>.
34. "Boundless Informant: NSA Explainer-Full Document Text," *Guardian*, June 8, 2013, <http://guardian.co.uk>.
35. Glenn Greenwald, "XKeyscore: NSA Tool Collects 'Nearly Everything A User Does On the Internet,'" *Guardian*, July 31, 2013, <http://theguardian.com/>
36. "DCSNet," accessed May 30, 2014, <http://en.wikipedia.org>.
37. "EFF Documents Shed Light on FBI Electronic Surveillance Technology," August 29, 2007, <http://eff.org>.
38. Susan M. Menke, "Army Guard and FBI Sign Up for less IP net," October 23, 2003, <http://gcn.com>.
39. "Carnivore (software)," accessed May 30, 2014, <http://en.wikipedia.org>.
40. Leslie Cauley, "NSA has Has Massive Database of Americans' Phone Calls," *USA TODAY*, May 11, 2006, <http://usatoday30.usatoday.com>.
41. "AT&T's Role in Dragnet Surveillance of Millions of its Customers," <https://eff.org>.
42. *In re Nat'l Sec. Agency Telecomms. Records Litig. (Hepting v. AT&T Corp.)*, 671 F.3d 881, (9th Cir. 2011), <http://www2.bloomberglaw.com>.
43. Associated Press, "Pentagon To Shut Down Controversial Database," August 21, 2007, <http://nbcnews.com>.
44. U.S. Department of Justice, Office of the Inspector General, "The Federal Bureau of Investigation's Terrorist Threat and Suspicious Incident Tracking System, Audit Report 09-02," November 2008, <http://justice.gov>.
45. "Homeland Security Revives Supersnoop," *Washington Times*, March 8, 2007, <http://washingtontimes.com>.
46. Bob Sullivan, "FBI Software cracks Cracks Encryption Wall," November 20, 2001, <http://nbcnews.com>; "Keystroke logging," accessed May 30, 2014, <http://en.wikipedia.org>.
47. "Trojan horse (computing)," accessed May 30, 2014, <http://en.wikipedia.org>.
48. Timothy B. Lee, "Five Ways To Stop the NSA From Spying On You," *Washington Post*, June 10, 2013, <http://washingtonpost.com>.
49. "What is the Tor Browser Bundle?," (with instructions for use), <https://torproject.org>.
50. "Off-the-Record Messaging," <http://cyberpunks.ca/otr>.
51. "Silent Circle, The World's Most Secure Solution in Mobile Privacy," <https://silentcircle.com>; "Red Phone :: Secure Calls," October 21, 2013, <https://play.google.com/store/apps>.
52. "Mobile phone tracking," accessed May 30, 2104, <http://en.wikipedia.org>.
53. "Riseup.net Security Resources," <https://riseup.net/en/resources>.
54. Kevin Gostola, "Lawsuit: Attempted Entrapment of Activists by Military Officer & Further Evidence of Domestic Spying," February 26, 2014, <http://dissenter.fire-doglake.com>.
55. *Support Eric McDavid*, <http://support-eric.org>.
56. Dana Priest and William M. Arkin, "A Hidden World, Growing Beyond Control," *Washington Post*, July 19, 2010, <http://projects.washingtonpost.com>.
57. Adam Federman, "We're Being Watched: How Corporations and Law Enforcement Are Spying on Environmentalists," *Earth Island Journal*, Summer 2013, <http://earthisland.org>.
58. *Ibid.*
59. See Thermis, "Information Operations Recommendation," November 29, 2010, <http://images2.americanprogress.org>.
60. See <http://boldnebraska.org> for more information about the FOIA documents this group unveiled.
61. *Tar Sands Blockade*, <http://tarsands-blockade.org>.