International Journal of Communication 10(2016), 1721–1742 1932–8036/20160005

Jus Algoritmi: How the National Security Agency Remade Citizenship

JOHN CHENEY-LIPPOLD
University of Michigan, USA

Classified U.S. National Security Agency (NSA) documents released in the summer of 2013 detailed a trove of controversial surveillance programs, igniting a debate about state power and the rights of citizens. But how can citizenship be evaluated in a digital, networked world? In response to this question, the NSA created an algorithmic, data-based version of citizenship (and foreignness), where a user is legally foreign if his or her "selectors" are "at least 51 percent confidence" foreign. These selectors, which can include telephone numbers, Internet protocol addresses, or language, became effectual arbiters of citizenship online. This article explains what algorithmic citizenship means, what the NSA's citizenship and foreignness look like, and what the implications are when a formal rubric of U.S. citizenship is based exclusively on algorithmic interpretations of communications data.

Keywords: NSA, citizenship, algorithm, data, privacy, surveillance, state power

By now, it is a familiar story. In May 2013, Edward Snowden landed in Hong Kong with four laptops in tow. On those laptops were tens of thousands of classified documents detailing the U.S. National Security Agency's (NSA) global ubiquitous surveillant assemblage and its "collect it all" approach to data acquisition (Cohn & Timm, 2013). The technicalities of the NSA's spying apparatus were awe-inducing: Most of the world's communication packets were, at the very least, open to being intercepted and saved into an NSA database. E-mails, search queries, metadata, and even screenshots of video chats were being recorded without people's knowledge (Ackerman & Ball, 2014; Greenwald & Ackerman, 2013). The U.S. government was trying to capture the world's data and save it for an undetermined period of time.

Included in these Snowden-leaked documents was a collection of secret legal briefs, memos, and court decisions outlining the legal foundations that justified the NSA's global surveillance network. These documents revealed how the U.S. state negotiates its ubiquitous surveillance program while simultaneously—and allegedly—respecting the privacy protections afforded to U.S. citizens by the U.S. Constitution's Fourth Amendment. Ultimately, this negotiation centered on a single, overarching question: How does one determine citizenship online?

John Cheney-Lippold: jchl@umich.edu
Date submitted: 2015–08–02

Copyright © 2016 (John Cheney-Lippold). Licensed under the Creative Commons Attribution Non-commercial No Derivatives (by-nc-nd). Available at http://ijoc.org.

Historically, the citizen—the subject of more than a century of privacy law—was an identifiable individual. She was a unique person with a name and a body who could be assigned the status of citizen or foreigner based on existing credentials. These credentials originated from the political legacies of either *jus sanguinis* or *jus soli* (Brubaker, 1992; Henriques & Schuster, 1917). If an individual was a citizen according to *jus sanguinis*, it was because her blood carried her citizenship—if one's parent or spouse was a citizen of a country, one became a citizen, too. If an individual was a citizen according to *jus soli*, it was because her birth founded her citizenship—if one was born in a country, one became a citizen of that country. The eventual artifact that proves citizenship, be it a birth certificate, passport, or state-issued identity card, is derived from one or both of these bona fides. As verified government documents, these artifacts confer onto individuals the right to formal citizenship (Torpey, 2000).

But online, people possess no government documents. When mediated through the technologies that compose the Internet, the identifiable, individual citizen is unrecognizable. The same technologies that facilitate ubiquitous surveillance also make it impossible to understand with certainty who is and who is not a citizen of the United States. An Internet protocol (IP) address, such as 93.45.225.191, is just a location for transmission control protocol packets to be sent to and from a device. A unique media access control address for a phone or computer, such as 00-50-5A-46-18-C1, is merely an identifier for network interface hardware. Neither has a political character, and neither is permanent; thus, neither has the ability to establish one's *jus sanguinis* or *jus soli* right to citizenship. User profiles, e-mail accounts, and even Facebook pages are all functionally disconnected from a singular, rights-bearing self.[1]

Without a unique index to assign as either citizen or foreigner, the NSA was at a legal impasse. If the NSA really wanted to "collect it all," how could it protect U.S. citizens from this global dragnet? Online, the NSA was unable to rely on historical conceptions and theories of the citizen and was thus unable to understand who was, and was not, constitutionally off limits for surveillance. But rather than shut down its massive surveillance network, the U.S. government instead created a new, ad hoc legal standard of citizenship.

This standard is based on the data people produce on the Internet—the messages they send, the language they use, the friends they have—that signal to an NSA computer and analyst the quantitative degree of how foreign (and inversely, how citizen) a user is. If an individual's foreignness is found to be at or above "51 percent confidence" (Gellman & Poitras, 2013, "Roots in the '70s" section, para. 6), then that individual legally becomes a foreigner and thus loses the right to privacy. This is what I call *jus algoritmi*, or citizenship rights according to algorithmic logic. Unlike its *jus soli* and *jus sanguinis* predecessors, *jus algoritmi* is not a category that confers membership within an imagined national body politic. It is not something that we know about, nor something we can identify as. It is instead a (once-) secret framework that extends the legal reach of NSA surveillance into the depths of the Internet—and into the jurisdiction

[1] Although Facebook and Google tried to enforce a singular identity onto Internet accounts, this singular identity cannot fully map onto a unique individual identity, because different people may use the same Facebook account, and a full name on a Google profile is not necessarily, nor legally, the real name of the person using the account (Lingel & Golub, 2015).

of "collect it all."

In this framework we move further toward what I have previously called "a new algorithmic identity" (Cheney-Lippold, 2011, p. 164). This identity, based on how algorithmic logic makes data about people useful, is different from how people have historically understood themselves as having identity—in this case, citizen identity. The algorithmic citizenship of *jus algoritmi* is a citizenship of technical requirement, one that can neither be intentionally practiced nor remain functionally stable. *Jus algoritmi* is instead a dynamic, temporal interpretation, similar to what Johanna Drucker and Bethany Nowviskie (2004) describe as "speculative computing," which "suggests that the concrete be replaced by plasticine that remains malleable, receptive to the trace of interpretive moves" (p. 433).

In this article, I summarize the NSA surveillance leaks and detail some of the key legal events that frame how contemporary state surveillance operates in the United States. Then I expand on the concept of *jus algoritmi*, how it functions, and what constitutes an algorithmic foreigner and algorithmic citizen according to leaked legal documents. I conclude with a discussion on what a shift to *jus algoritmi* means for the concept of citizenship itself. Algorithmic citizenship is not a citizenship in ways we previously conceived. Instead, it is a data-based method by which the NSA can fulfill its legal obligations while maintaining its extensive surveillance apparatus.

The Snowden Leaks, the Fourth Amendment, and Warrantless Wiretapping

In 2005, General Keith Alexander became the director of the NSA. Continuing the trend that had defined the agency's preceding decade, Alexander pushed for an even faster acceleration of signal intelligence acquisition. Instead of targeting and surveilling only those individuals whom the U.S. state surmised to be suspicious, the NSA would, in its own words, "collect it all" (see Figure 1). As described by a former senior U.S. intelligence official, "Rather than look for a single needle in the haystack, [Alexander's] approach was, 'Let's collect the whole haystack' . . . 'Collect it all, tag it, store it. . . . And whatever it is you want, you go searching for it'" (Nakashima & Warrick, 2013, para. 3). "Collect it all" became the mantra of the Alexander-era NSA, and enacting this mantra required an extensive apparatus for surveillance.

In 2013, this apparatus was gradually revealed in the waves of NSA-related journalism following the Snowden leaks. The resulting reports detailed the U.S. government's incredible capacity to surveil the globe's communication networks. Secret programs once known by a select few in the U.S. intelligence community quickly became household names. Code name after code name, the hidden interior of the NSA's collect-it-all surveillance assemblage was laid bare. Although this assemblage was both overly intricate and described using opaque, technocratic language, the reach of NSA surveillance can be better understood by dividing its practical execution into two separate camps: upstream and downstream data collection.[2]

[2] I refer to NSA programs and activities in the past tense because Snowden's materials are almost three years old at the date of this publication.

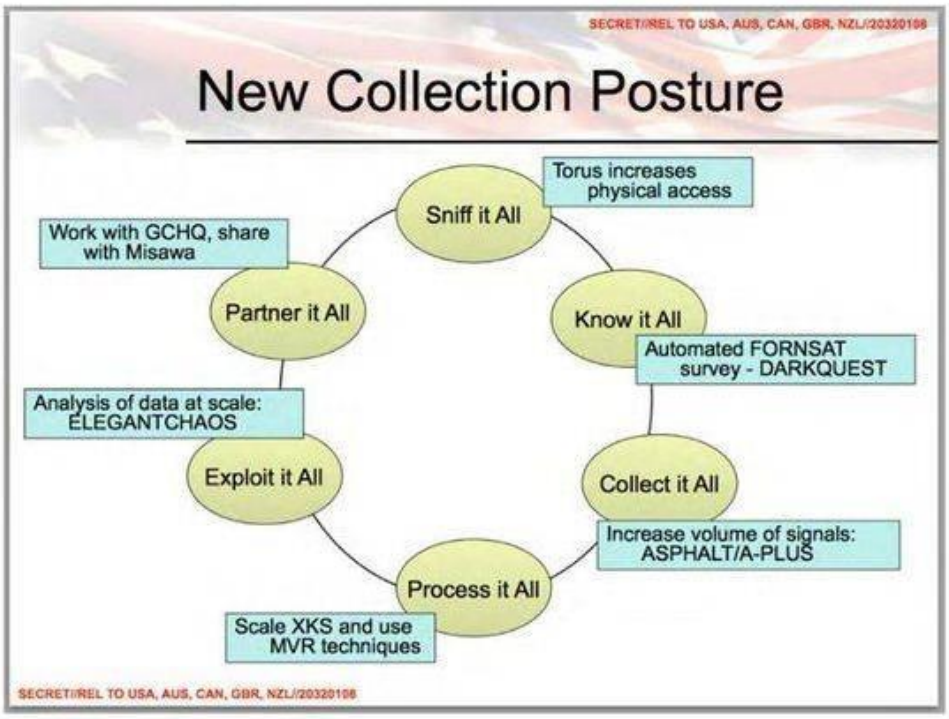

Figure 1. A slide illustrating the NSA's "collect it all" approach. From National Security Agency (2014).

Upstream data came from active network traffic, or what the NSA defined as "communications on fiber cables and infrastructure as data flows past" (National Security Agency, 2013, p. 3; see Figure 2). A hypothetical Web query from a computer in Ann Arbor, Michigan, to the German newspaper *Der Spiegel* would cross a dozen routers, pass through several network backbones, and even travel on a fiber-optic cable laid on the bed of the Atlantic Ocean. To capture this query, the NSA, as described in programs such as Fairview, Mystic, Blarney, Oakstar, and Stormbrew, would tap into key points of the Internet's infrastructure and copy all traffic that passed through them.[3] By aggregating upstream data into central NSA servers, the U.S. intelligence community assembled a real-time reservoir of much of the world's Internet network communications, providing NSA analysts a significant portion of the Internet's data in searchable, pattern-analyzable form.

[3] Fairview gathered bulk phone and Internet data from various foreign telephone and Internet providers. Mystic recorded every phone call made in either Iraq or the Bahamas and Afghanistan, saving each as an audio file for, allegedly, 30 days. And Blarney, Oakstar, and Stormbrew were nominally separate programs that tapped directly into high-traffic fiber-optic cable hubs and other communications infrastructure (Timberg, 2013).

Figure 2. A slide detailing PRISM's upstream and downstream collection. From National Security Agency (2013, p. 3).

Downstream data came from access to commercial and nongovernmental servers under the PRISM program, or what the NSA defined as data collected "directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, Apple" (National Security Agency, 2013, p. 3). Under PRISM, NSA and Federal Bureau of Investigation computers were able to directly tap into these companies' cloud-based servers to extract "audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets" (Gellman & Poitras, 2013, para. 1).

Almost all this data interfaced with a program called XKeyscore, the portal through which NSA analysts could sift through the agency's gigantic databases full of the world's downstream and upstream data flows (Greenwald, 2013). Described by Snowden as the NSA's "front end search engine," XKeyscore served, much like Google does for the superficial Web, as a query-based access point for the near-totality of the U.S. government's data cache (Norddeutscher Rundfunk, 2014, para. 4). XKeyscore gave analysts unregulated access to almost all the data collected by instances of U.S. state surveillance—from the communications of the U.S. president to those of federal judges and foreign leaders.

With such expansive surveillance capacities came an obligatory legal concern: How could this type of ubiquitous data collection be found constitutional? Wiretaps on both upstream and downstream data would inevitably mean that U.S. citizens' information was harvested into an NSA database. It seems to be functionally unworkable for the NSA's collect-it-all mission and wiretaps to square with the letter of the law spelled out by the U.S. Constitution's Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Most interpretations of this amendment require that searches be accompanied by a corresponding warrant. Instances that are "reasonable," and that do not require a warrant, usually engage with questions of public space, probable cause, and exigent circumstances (Amsterdam, 1974; Mascolo, 1972). But, as Akhil Reed Amar (1994) argues, there is an abundant inconsistency in how the courts treat warrants, probable cause, and the exclusion of illegally obtained evidence. He explains, "The Fourth Amendment today is an embarrassment. . . . Much of what the Supreme Court has said in the last half century . . . is initially plausible but ultimately misguided" (p. 757).

Legal theorists have identified this inconsistency both in the off-line, physical environment as well as in the increasingly technologically networked world (Burkoff, 1979; Maclin, 1998). Most notably, Orin Kerr (2011) writes that the Fourth Amendment "consists of dozens of rules for very specific situations that seem to lack a coherent explanation. Constitutional protection varies dramatically based on seemingly arcane distinction. . . . Fourth Amendment rules can appear to be selected almost at random" (pp. 479–480). And there is still controversy "over whether the warrant requirement to the Fourth Amendment applies to surveillance of American citizens overseas" (Forgang, 2009, p. 222). This controversy grows even more contentious when it remains unknown whether a person is a citizen and whether that citizen is overseas.

To more fully understand this legal structure in terms of NSA surveillance, we can look to a sequence of events in U.S. surveillance law beginning with the 1978 Foreign Intelligence Surveillance Act (FISA). Historically, this act served as the legal mediator between the reach of U.S. spycraft and the protections guaranteed to U.S. citizens under the Fourth Amendment (Cinquegrana, 1989). But, as mentioned above, surveillance on an individual body is different than surveillance on a phone. A single phone may be used by several different people over the course of a day, making it nearly impossible to positively identify an individual voice as the intended target for surveillance. In acknowledgment of this limitation, FISA required the government to have only "probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power" to begin monitoring that target's communications (50 U.S. Code § 1805). In lieu of decisive identification, FISA provided the NSA legal flexibility through the phrase "probable cause."

Fast-forward to October 2001 and the introduction of the USA PATRIOT Act. Well known as the post-9/11 exemplar of reducing civil liberties in the name of national security, the act gave blanket powers

to the Bush administration, and future members of the executive branch, to surveil most individuals without warrants, often without probable cause, and without any meaningful oversight (Whitehead & Aden, 2002). More specifically, the act contained a loophole that theoretically allowed the government to circumvent FISA's probable cause requirement even when the main purpose of a search was entirely unrelated to foreign intelligence (Funk, 2007; Sullivan, 2014).

The specifics of this warrantless surveillance enabled by the PATRIOT Act's legal framework were kept secret until a 2006 *Wired* story about wiretapping at a San Francisco AT&T telecommunications facility. In this case, the NSA had tapped into domestic upstream data at a primary AT&T Internet backbone in San Francisco, California (Singel, 2006). In response to the outcry and purported unconstitutionality of these NSA wiretaps, the Bush administration pushed the 2008 FISA Amendments Act through Congress.

The 2008 Amendments Act overwrote requirements for probable cause, individual suspicion, or even warrants, thereby authorizing surveillance on any foreigner "reasonably believed to be located outside the United States" (50 U.S. Code § 1881a). Any noncitizen deemed outside the United States was at risk of being surveilled, regardless of whether she or she was actually a foreign agent. This also, quite saliently, would include citizens who communicated with noncitizens deemed outside the United States.

Yet the act left undefined what constitutes a U.S. citizen, or, in the parlance of U.S. federal law, what makes a "United States person"—which includes citizens, legal permanent resident aliens, and corporations incorporated in the United States (U.S. Code § 6010). According to publicly available legal documents, a United States person is, tautologically, anyone who can prove his or her U.S. personhood through a state-authenticated artifact of citizenship, green card, or articles of incorporation. Conversely, a non–United States person is anyone unable to provide such documentation.

But conventional proof of citizenship status through documentation is nonviable in a digitally networked world, a point made explicit in a 2009 classified document by the U.S. Foreign Intelligence Surveillance Court (the court responsible for FISA surveillance) leaked by Snowden. For the purposes of this article, "Exhibit B: Procedures Used by the NSA in Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" defines a United States person in two ways:

> (1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the *nature or circumstances of the person's communications give rise to a reasonable belief* that such person *is not* a United States person.
>
> (2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as United States person unless such person can be positively identified as such, or the *nature or circumstances of the person's communications give rise to a reasonable belief* that such person *is* a United States person. (Holder, 2009b, p. 2; emphasis mine)

These two definitions recall the 2008 FISA Amendments Act phrasing of "reasonable belief." In the first definition, an individual is a United States person as long as she stays in the United States and does not produce "reasonable belief" that she is not a United States person. Thus, if an individual leaves the United States, she is no longer a United States person by default, even if she is a citizen. And although everyone located in the United States is officially considered a United States person by default, an individual remains a United States person only if her communication data provokes no "reasonable belief" that she is foreign. Ultimately, the U.S. state's interpretation of an individual's communications data can identify the person as *not a United States person*, and thus create the legal framework for *"reasonable belief" foreignness*.

In the second definition, an individual outside the United States—or one "whose location is unknown"—is not a United States person as long as she stays outside the United States, produces no location-identifying information, and does not produce "reasonable belief" that she is a United States person. But with this definition we should emphasize two things. First, all data traffic is, technologically, location-unknown. Although IP addresses are often assigned geographic identities, there is no exact relation between an IP address and a person's geographic location. Second, although everyone outside the United States (or location unknown) is considered a non–United States person, an individual remains a non–United States person as long as there is no "reasonable belief" in her communication data that she is a United States person. Ultimately, the U.S. state's interpretation of an individual's communications data also arbitrates her as a *United States person*, and thus creates the legal framework for *"reasonable belief" citizenship*.

This phraseology of "reasonable belief" became the legal foundation that post-2009 U.S. government officials would subsequently employ to differentiate noncitizens from citizens online. Instead of requiring that a surveillance subject be a locatable and provable "foreign agent," the U.S. intelligence community could now spy on those who were, according to the above two definitions, both reasonably believed to be a foreigner and not reasonably believed to be a citizen.

For example, take two hypothetical people: Person X and Person Y. X's computer is connected to an IP address in Ann Arbor, Michigan. Y's computer is connected to an IP address in Managua, Nicaragua. At face value, X is a citizen and Y is a foreigner. But as each user[4] produces additional communications data—e-mails, search queries, even new friends on Facebook—that data, and its "reasonable belief" value, becomes the primary variable that determines the user's status as citizen or foreign. If X were to produce data reasonably believed to be foreign, X would stop being a citizen and become a foreigner. If Y were to produce data reasonably believed to be citizen, Y would stop being a foreigner and become a citizen.

As we learned from the Snowden leaks, this interpretation of citizenship was imperfect, but it produced a relation to citizenship that facilitated, rather than constrained, the collect-it-all approach of the

[4] For the remainder of this essay, I will no longer refer to "persons" or "individuals." In terms of NSA spycraft, an individual person who produces data is unavailable for identification. Rather, we should think of a "user" as a person/persons who produce data believed to be produced by a single person.

Alexander-era NSA. With reasonable belief, virtually anyone, citizen or not, could be perceived as foreign enough to legally justify surveillance. And indeed, the only constant in this *jus algoritmi* formulation is the process by which an NSA computer and/or analyst operationalizes reasonable belief. The primary questions then become: How is reasonable belief operationalized, and how is algorithmic foreignness and algorithmic citizenship distributed?

Foreignness, 51%, and *Jus Algoritmi*

For the data-obsessed NSA, reasonable belief is an empirical measurement: a procedural interpretation of data according to a set of preexisting criteria. And this interpretation becomes *the* interpretation of a user's U.S. personhood online—and thus determines whether that user has the legal status to enjoy the constitutional right to privacy. As argued by Hallinan and Striphas (2014) in their study of the Netflix recommendation algorithm, algorithmic processing is a form of "cultural decision making" (p. 119). With the NSA's *jus algoritmi*, algorithmic processing is a form of legal decision making, too.

This decision making comes in the form of a quantitative confidence measure. A *Washington Post* analysis of the downstream "PRISM Tasking Process" notes that the NSA instructed "analysts who use the system from a Web portal at Fort Meade, Md., [to] key in 'selectors,' or search terms, that are designed to produce at least 51 percent confidence in a target's 'foreignness'" (Gellman & Poitras, 2013, "Roots in the '70s" section, para. 6). In other words , if a target reaches at least 51% confidence, then she is "reasonably believed" to be, and thus actionably becomes, a non–United States person—and thus a foreigner. And as a foreigner, the user is denied any Fourth Amendment protection of privacy.

The "51% confidence" standard is to *jus algoritmi* as a blood quantum measurement is to *jus sanguinis* and a birth certificate is to *jus soli*. But unlike the materiality that articulates one's *sanguinis* or *soli* belonging, like blood or birthplace, the materiality of *jus algoritmi* is a stream of data flowing through fiber-optic cables under the ocean and in the cloud server farms of companies such as Google. These data are then distributed into the dual frameworks of reasonable belief citizen or reasonable belief foreigner according to the NSA's algorithmic logic.

Importantly, the exact process by which this distribution takes place remains unknown. As it stands, I have intentionally implicated both NSA computers and NSA analysts as agents within the framework of *jus algoritmi*, because 51% confidence signals an instance of interpretation, using algorithmic logic, by a computer and/or an analyst. By this I mean that, although it is possible that NSA computers assign users' IP addresses, media access control addresses, or e-mail accounts a running, real-time quantitative foreignness score, I also want to emphasize the similar possibility of an NSA analyst looking at available data, quantitatively evaluating its foreignness and citizenness, and then making a subsequent, human-based claim that a user is foreign by at least 51% confidence.

Automated or not, the logic of *jus algoritmi* produces a new legal relation between people, their data, the U.S. state, and the concept of citizen. To phrase it differently, *jus algoritmi* is a formal, state-sanctioned enaction of citizenship that distributes political rights according to the NSA's interpretations of data. As discussed later, the messy, lived realities of citizenship never perfectly align with the political

promises prescribed by one's birth certificate. The U.S. state has historically regulated what kinds of people can enjoy the practices of citizenship, regardless of their formal status as citizens. For example, non-White racial groups and immigrants are often neither seen nor treated as full citizens, despite possessing U.S. birth certificates, passports, or certificates of naturalization. *Jus algoritmi*'s logic enshrines this functional arbitrariness of citizenship—and its subsequent precarity—into an actionable legal standard.

This legal standard is what the U.S. government secretly referred to as a "foreignness determination" (Holder, 2009a, p. 1). Such determinations are made explicit in a Snowden-leaked document explaining how *jus algoritmi* operationally functions. Former U.S. Attorney General Eric Holder's 2009 "Exhibit A: Procedures Used by the NSA in Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended" outlines a long list of factors the NSA can use to reach 51% confidence in making a judgment of foreignness. For telephone communications, one is viewed as more likely to be foreign than citizen if, as stated above, one's metadata "reveals that [one's] telephone number is used by an individual associated with a foreign power or foreign territory" (Holder, 2009a, p. 4). One is additionally likely to be viewed as foreign if one's "telephone number has been used to communicate directly with another telephone number reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory" (Holder, 2009a, p. 4). An individual might be even more likely foreign if that telephone number "communicated directly with an individual reasonably believed . . . to be used by an individual associated with a foreign power or foreign territory" (Holder, 2009a, p. 4). Importantly, all these determinations are dependent on whether a user is in contact with a foreigner—yet that foreigner needs only to be viewed as foreign by 51% confidence. This lack of a fixed sense of foreignness means everyone, theoretically, could be algorithmically read as foreign.

More interesting still is how different Internet communication factors are valued as foreign. As shown in Figures 3 and 4, a user might be considered more likely to be foreign if "information indicates that a user of the electronic communications account/address/identifier has communicated directly with an individual reasonably believed to be associated with a foreign power or foreign territory" (Holder, 2009a, p. 5). This means that a user might be viewed as a foreigner if she talks to a 51% confidence foreigner, or a user's "account/address/identifier is included in the 'buddy list' or address book of an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory" (Holder, 2009a, p. 5). Thus, a user might be additionally viewed as foreign if she talks to a 51% confidence foreigner who then adds the user to her Gchat contact list. And, similar to the original definitions of a reasonable belief foreigner, a user might be considered a foreigner if her IP address is "used almost exclusively by individuals associated with a foreign power or foreign territory." Or a user might be viewed as a foreigner if she uses cryptology or steganography "used almost exclusively by individuals associated with a foreign power or foreign territory" (Holder, 2009a, p. 5).

b. With respect to Internet communications:

- Information indicates that the electronic communications account/address/identifier has been used to communicate directly with an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
- Information indicates that a user of the electronic communications account/address/ identifier has communicated directly with an individual reasonably believed to be associated with a foreign power or foreign territory;
- Information indicates that the electronic communications account/address/identifier is included in the "buddy list" or address book of an electronic communications account/address/identifier reasonably believed by the U.S. Intelligence Community to be used by an individual associated with a foreign power or foreign territory;
- Information indicates that the electronic communications account/address/identifier has been transmitted during a telephone call or other communication with an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;
- Public Internet postings match the electronic communications account/address/ identifier to an individual reasonably believed by the U.S. Intelligence Community to be associated with a foreign power or foreign territory;

Figure 3. Exhibit A minimization procedures. From Holder (2009a, p. 5).

More daring still, Snowden documents leaked to the Brazilian newspaper *O Globo* describe how the XKeyscore program detects "the presence of foreigners according to the use of language in emails and phone calls" (Greenwald, Kaz, & Casado, 2013, para. 1). The centuries-old, nationalist refrain of "one state, one nation, one language" is reaffirmed in the Internet era when the act of speaking a language other than English suggests a user might be more foreign than citizen (May, 2001, p. 94). The resulting inverse of the ideal foreigner—the ideal citizen—is a user who never calls, e-mails, or makes it into the address book of another user who is a foreigner; never travels outside the United States; and speaks exclusively English, to other English speakers, without encryption.

- Information contained in various NSA-maintained knowledge databases of foreign intelligence information acquired by any lawful means, such as electronic surveillance, physical search, the use of a pen register or trap and trace device, or other information, reveals that electronic communications account/address/identifier has been previously used by an individual associated with a foreign power or foreign territory;

- Information made available to NSA analysts as a result of processing metadata records acquired by any lawful means, such as electronic surveillance, physical search, or the use of a pen register or trap and trace device, or other information, reveals that the electronic communications account/address/identifier is used by an individual associated with a foreign power or foreign territory; or

- Information indicates that Internet Protocol ranges and/or specific electronic identifiers or signatures (e.g., specific types of cryptology or steganography) are used almost exclusively by individuals associated with a foreign power or foreign territory, or are extensively used by individuals associated with a foreign power or foreign territory.

Figure 4. Exhibit A minimization procedures, continued. From Holder (2009a, p. 5).

So how does the NSA determine one's algorithmic citizenship? First, we must understand that the above criteria, used to establish *jus algoritmi* through foreignness determination, are metadata. Metadata are data about data, or, in a postal metaphor, they are the data that would be found on the outside of an envelope. Users produce this data every time they make a query on the Internet, be it an e-mail, a Web page request, or any other protocol of Internet communication. For example, an HTTP request from Ann Arbor, Michigan, to Google.com can look like this:

```
GET /dumprequest HTTP/1.1
Host: google.com
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_1) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/46.0.2490.86 Safari/537.36
DNT: 1
Referer: https://www.google.com/
Accept-Language: en-U.S.,en;q=0.8,es;q=0.6
```

Second, these metadata are transferred across several different routers across the country. From Ann Arbor, Michigan, the program Traceroute can be used to see how it traveled to Google's servers in Mountain View, California:

traceroute to google.com (173.194.46.99), 64 hops max, 52 byte packets
1 192.168.1.1 (192.168.1.1) 2.136 ms 10.605 ms 1.822 ms
2 XX.XXX.XX.XXX (XX.XXX.XX.XXX) 20.493 ms 14.788 ms 10.868 ms
3 te-4-1-ur02.nannarbor.mi.michigan.comcast.net (68.86.120.69) 11.732 ms 18.783 ms 12.182 ms
4 te-0-5-0-6-ar02.taylor.mi.michigan.comcast.net (68.87.190.149) 13.984 ms 11.620 ms 20.613 ms
5 te-0-7-0-2-ar02.pontiac.mi.michigan.comcast.net (68.87.191.114) 14.778 ms 13.350 ms
te-0-7-0-5-ar02.pontiac.mi.michigan.comcast.net (162.151.20.166) 20.382 ms
6 be-33668-cr02.350ecermak.il.ibone.comcast.net (68.86.90.45) 23.908 ms 22.665 ms 20.294 ms
7 metainterfaces-cr01.sanjose.ca.ibone.comcast.net (68.86.89.142) 19.063 ms 21.766 ms 21.746 ms
8 as15169-3-c.350ecermak.il.ibone.comcast.net (173.167.57.210) 67.389 ms 65.685 ms 60.691 ms
9 209.85.244.3 (209.85.244.3) 24.082 ms 24.939 ms 19.865 ms
10 209.85.245.225 (209.85.245.225) 21.652 ms 19.540 ms 19.579 ms
11 ord08s13-in-f3.1e100.net (173.194.46.99) 25.791 ms 35.079 ms 33.648 ms

Figure 5. A screenshot from IXmaps (ixmaps.ca).

At each of these "hops" is a router. And each router has the capacity to record each HTTP request that passes through it. This is the material place, the physical node, where an NSA wiretap might collect upstream data. To better understand how this network architecture might connect to NSA surveillance wiretaps, we can use a tool called IXmaps (see Figure 5). IXmaps makes use of Traceroute's capabilities and overlays each voyage across the Internet with a continually curated set of new knowledges about where NSA wiretaps are likely to be. IXmaps lets people "see where your packets go," both in terms of how a person's traffic gets from Ann Arbor to Google, and how probable it is that a certain TCP/IP request will pass through one of the alleged NSA wiretaps points—estimated to number about 40 within the continental United States (Clement, McCann, Resch, & Stewart, 2012).

Ultimately, with this metadata logged into an NSA database, the technical structures of NSA surveillance can be connected to the interpretative logic of *jus algoritmi*, wherein an NSA computer or analyst would evaluate this data according to the above foreignness determination criteria. A creative exposition of this evaluation is available in *Citizen Ex*, a software art project by James Bridle (2015) based on my earlier research around the concept of *jus algoritmi*. This browser extension considers some of the NSA's foreignness confidence-producing elements (e.g., talking to a foreigner, having a foreign IP address) and generates an algorithmic, percentage assessment of a user's citizenship. The extension follows the user's history of Internet Web traffic, recording the assumed, geographic location of her computer at the moment of a Web page request and the assumed, geographic location of the server that receives the user's request. For example, our single request from Ann Arbor, Michigan, to Google.com gives us 100% confidence U.S. citizenship. But add to that another request to *Der Spiegel* (whose servers are in Hoest, Germany) and one's algorithmic citizenship gets reconfigured: One is now 75% U.S. and 25% German (see Figure 6). Citizenship becomes arbitrarily dependent on the algorithmic interpretations of the Web sites we currently are visiting.

To quickly overview, *jus algoritmi* is an algorithmic identity whereby a user is differentially assigned categorical membership as citizen or foreigner according to that user's processed data. This identity may functionally value that user as 51% confidence likely to be a citizen in the eyes of the NSA when that user is actually a foreigner, or 51% confidence likely to be a foreigner in the eyes of the NSA when that user is actually a citizen. Yet the seeming contradiction between one's algorithmic citizenship and one's formal citizenship is concealed by the fact that users will never know whether the NSA considers them citizens or foreigners of the United States, nor will users directly feel the sway of subsequent privacy invasions. Indeed, the entirety of the *jus algoritmi* legal apparatus wants it that way—hence the bold "TOP SECRET" adorning leaked NSA documents and the fact that the Exhibit A and Exhibit B minimization procedures documents are both "classified until 2032" (Holder, 2009a, p. 1; Holder, 2009b, p. 1).

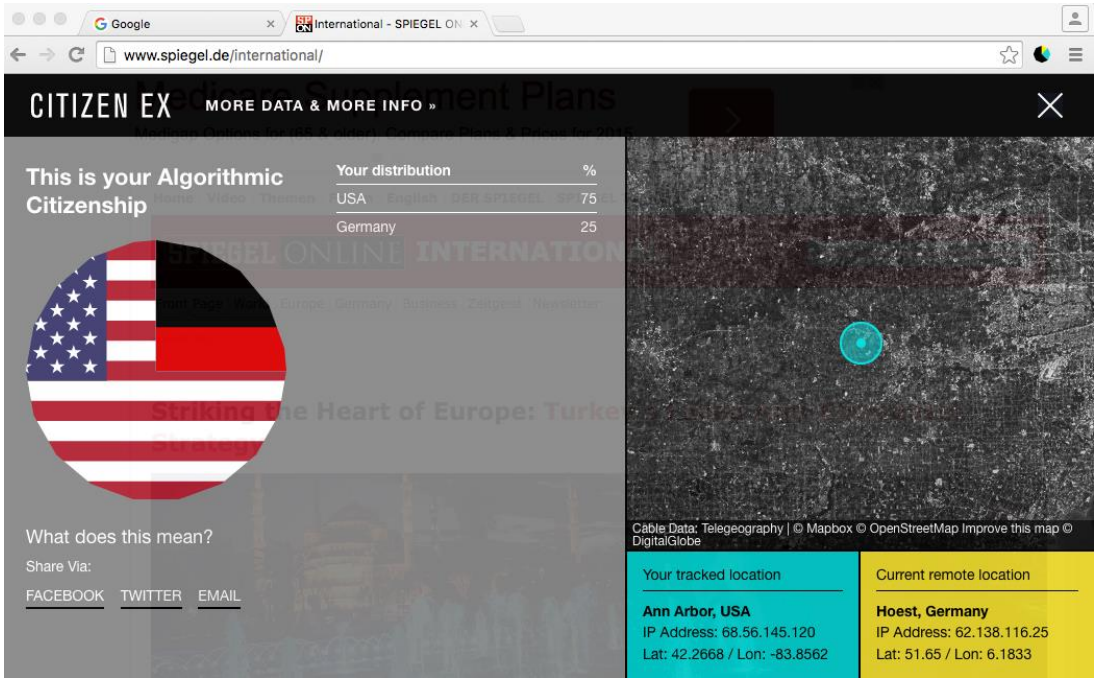

Figure 6. A screenshot from James Bridle's Citizen Ex.

Citizenship

It is through this hidden logic that we see how *jus algoritmi* constructs a citizenship that exclusively aims to fulfill the legal mandate of U.S. constitutional precedence while supporting the NSA's collect-it-all approach. And as a new construction it is both distinct from and similar to its nonalgorithmic conceptual cousin.

The distinction comes from algorithmic citizenship's relationship to the political reflexivity implicit in citizenship's nonalgorithmic form. Consider Hannah Arendt's (1973) famous slogan describing the status of belonging to a nation-state: the "right to have rights" (p. 296). In this oft-quoted passage, Arendt discusses the human right to membership in a political community. But immediately following this claim is an addendum to the right to have rights: "(and that means to live in a framework where one is judged by one's action and opinions)" (pp. 296–297). In this traditional definition of citizenship, to be member of a political community meant one actively belonged not as an abstract constituent but as a participant of the body politic. Being a citizen, then, involved acting and being judged by one's actions. Further, the community reacted according to those judgments.

This process of participation, judgment, and reaction by the community can be thought of as what Nikolas Rose (2009) calls a "citizenship project." Historical citizenship projects describe "the ways that authorities thought about (some) individuals as potential citizens, and the ways they tried to act upon

them" (p. 131). For example, Rose points to the definition of "those who were entitled to participate in the political affairs of a city or region" and the requirement for "citizens to speak a single national language," where "such citizenship projects were central both to the idea of the national state, and to the practical techniques of the formation of such states" (p. 131). The requisite acting upon individuals produced a regulatory framework for a model, national citizenry.

Jus algoritmi, though, does not participate in these types of citizenship projects. To be unknowing of one's membership in one's political community confounds the necessary reflexivity of this traditional type of citizenship. When a user is secretly seen as foreign, there is no empowered response or judgment that returns as feedback to the user. And although there remain clear racialized, ethnic, and cultural lenses through which the NSA makes its foreignness determinations, the consequence of *jus algoritmi* avoids direct involvement in the debate about what a national population looks like and identifies as. And because it is impossible to identify who is and who is not an algorithmic citizen, we have no way of interpreting how the NSA's algorithmic logic regulates membership into the national imaginary.

Having said that, *jus algoritmi*'s percentaged, incomplete mode of citizenship is operationally apropos to how the rights of a traditional citizen are discriminately allocated. Throughout the history of the United States, there have always been some individuals who are formally bestowed citizenship but who are prohibited from practicing that citizenship in a fully, 100% incorporated way. For instance, Mae Ngai (2014) writes of Asian immigrants into the United States as "impossible subjects," who, even after becoming U.S. citizens, are never seen as such due to their immigration status and ethnic identity. Edlie Wong (2015) describes the "fictions of citizenship" that reinforced the racial link between Whiteness and full citizenship in post-Reconstruction United States. And Patricia Hill Collins (2005) has extensively researched the racialized, gendered, and sexual foundations of U.S. citizenship standards that abruptly disavow the facile claims to political equality presupposed in most liberal democratic theory.

More practically, then, *jus algoritmi*'s citizenship is a functionalist variant of what C. Edwin Baker (2004) refers to as "corruption" of a social group, which "occurs when segmentation reflects the steering mechanisms of bureaucratic power or money rather than the group's needs and values" (p. 180). In this way, algorithmic citizenship mirrors how traditional, nonalgorithmic citizenship has never been guaranteed and universal, precisely because it is allocated according to needs of power. The algorithmic citizen is an identification of citizen-as-status according to data and a transcoding of existing legal limitations, not an identity that one can consciously refer or respond to, because its allocation is both hidden from the individual and changing at every moment.

So while *jus algoritmi* is clearly a form of citizenship imbued with discriminatory asymmetry (it marks non-U.S. IP addresses, non-English languages, and non-U.S. social networks as foreign), its theoretical standing is unlike Arendt's "right to have rights" and even unlike the racialized, gendered, and sexual regulations of the U.S. national imaginary. Rather, *jus algoritmi* is malleable, dynamic, and impermanent—it prevents any possible claim to inviolate protection in order to legally maintain the NSA's global collect-it-all surveillant assemblage. Its goal is not the maintenance of a White supremacist body politic but rather a functional instability of citizen status that theoretically enables any person to be momentarily perceived as foreign, and thus subject to U.S. state surveillance.

As a subject, the algorithmic citizen lives in the ether. Its legal and political positionality is deterritorialized from historical indices of citizenship in order to be reterritorialized according to the needs of the U.S. national security apparatus. One cannot declare "I am an algorithmic citizen" and expect political action or protection. In fact, leaked documents show that an NSA analyst who surveils a target later found to be a citizen has "nothing to worry about" (Gellman & Poitras, 2013, "Roots in the '70s" section, para. 6) from a legal standpoint.

Consequently, algorithmic citizenship is not really about rights; it is about a variable ordering of legal status for purposes of maintaining state power through the NSA's surveillant assemblage. One moment a user might be a citizen, the next that user might be a foreigner. As a container of discursive meaning, *jus algoritmi* operates exclusively via users' datafied behavior. The ideal of citizenship moves from some fixed source of determination (blood/birth, passport/birth certificate) and into a flexible assemblage of data that algorithmically become one's makeshift index for citizenship online. This ontological restructuring of citizenship according to data—instead of birth, lineage, or body—suggests that the potentiality of the algorithmic citizen is yet unknown. It is a citizenship that is always used against us, its motive disconnected from the liberal bourgeois history of citizenship as civic virtue. For the U.S. state, it is a tactical citizenship that rejects the ostensibly protective spirit of U.S. law in favor of the logistical needs of U.S. national security.

Cultural Politics of *Jus Algoritmi*

Although full citizenship in theory may not equal full citizenship in practice, the singular abstractions that emerge from *jus sanguinis* and *jus soli* still endure. But when algorithmic logic arbitrates what it means to be foreign and what it means to be a citizen, we witness a reframing of theoretical citizenship away from its traditional core and into a data-based form. This form, *jus algoritmi*, modifies not just the perceived essence of what makes a citizen but the character of citizenship itself. To be 51% confidence foreign means a user is also, to a lesser degree, citizen too. Unless a user is viewed as citizen or foreigner with 100% confidence (a statistical impossibility), that user will always be both. We are foreign and citizen at the same time, an empirical manifestation of *jus algoritmi* that makes no sense if we conceive of citizenship and foreignness in their *sanguinis* and *soli*—static and definitively comprehensive—terms. Like the discriminatory difficulties of living and practicing full citizenship in the real world, algorithmic citizenship is a legally empowered spectrum of citizen status located in the quantitative, and always-incomplete, in-between.

In this way, if a user is a *jus soli* citizen while the NSA labels that same user *jus algoritmi* foreign, we witness not misidentification but the corrupting reconstitution of the very idea of citizenship itself—a recasting of citizenship atop what Lev Manovich (2001) calls the data + algorithm ontology of the computer. This recasting rewrites citizenship into algorithmic terms, a corrupt but functional structure similar to what Antionette Rouvroy (2013) calls "data behaviourism," or the "new way of producing knowledge about future preferences attitudes, behaviours or events without considering the subject's psychological motivations, speeches or narratives, but rather relying on data" (p. 143). A confidence measure that dictates one's foreignness and citizenship marks a formative pivot in the arbitrary construction of both. Although political and cultural forces make all categories arbitrary in some way, a profound shift takes place when knowledges defining citizenship are produced through algorithmic logic.

This shift is characteristic of what Frank Pasquale (2015) describes as the "black box society." Users produce the datafied fodder that can algorithmically modulate their perceived citizenship and foreignness at each HTTP request, with each friend they talk to, and through each access point they log into. But although each datafied action has the possibility to realign the percentage confidence that a user is more foreigner than citizen or vice versa, we do not know how that percentage confidence is determined. A user's actions are weighed by an NSA computer and analyst, while the quantitative definitions of her algorithmic citizenship remain hidden.

Jus algoritmi functionally abandons citizenship in terms of national identity in order to privilege citizenship in terms of provisional interpretations of data. And the resulting partial citizenship of 51% confidence allows the operational logic of the NSA—collect it all—to become legally permissible. Everyone, whether a U.S. citizen or not, does things that could be deemed, under NSA minimization procedures, foreign. We talk to friends who are overseas, we speak non-English languages, we encrypt our communications, and we go on vacations outside the United States. Although some people, particularly immigrants and people with family outside the United States, enact these behaviors more than others, we all are potentially available to be *jus algoritmi* foreigners.

Significantly, the idealized index that theoretically founds a person's formal, official citizenship has transmuted from a seemingly stable object, such as a passport or birth certificate, into a data-based, shifting fount of performed citizenship. As a user's Internet habits change, that user also modulates her own degree of citizenship. *Jus sanguinis* and *jus soli* rely on the hypothetical constancy of state-based and state-authenticated archives. *Jus algoritmi* has no comparable archive. It relies instead on the massive flows of data sucked into the government's surveillance assemblage, where 51% confidence becomes the legal, albeit temporary, arbiter of protection against NSA surveillance.

This dynamic index of citizenship upends the static legal structure that enshrines the right to privacy. Similarly, this changing identity means people will be under constant evaluation according to the NSA's algorithmic logic, where analysts and computers assess users' datafied actions and distribute resources, rights, and life possibilities according to statistical interpretations of those actions. And, as more and more of our individual actions—who we talk to, where we are, what we search for, even what words we use in conversations—get datafied, more and more of who we thought we were in terms of citizenship is wrong. The algorithmic dialect of *jus algoritmi* might not know the vocabularies of passports or birth certificates, but it speaks fluently through fuzzy, data-based interpretations of what we do online. It is a distinct language of state affiliation, and, whether we want to or not, we are compelled to speak it.

References

Ackerman, S., & Ball, J. (2014, February 28). Optic nerve: Millions of Yahoo webcam images intercepted by GCHQ. *The Guardian.* Retrieved from http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

Amar, A. R. (1994). Fourth Amendment first principles. *Harvard Law Review*, *107*(4), 757–819.

Amsterdam, A. (1974). Perspectives on the Fourth Amendment. *Minnesota Law Review, 58*, 349–478.

Arendt, H. (1973). *The origins of totalitarianism*. New York, NY: Harcourt.

Baker, C. E. (2004). *Media, markets, and democracy*. Cambridge, UK: Cambridge University Press.

Bridle, J. (2015). Citizen ex. Retrieved from http://citizen-ex.com

Brubaker, R. (1992). *Citizenship and nationhood in France and Germany*. Cambridge, UK: Cambridge University Press.

Burkoff, J. (1979). The court that devoured the Fourth Amendment: The triumph of an inconsistent exclusionary doctrine. *Oregon Law Review*, *58*(2), 151–192.

Cheney-Lippold, J. (2011). A new algorithmic identity: Soft biopolitics and the modulation of control. *Theory, Culture & Society*, *28*(6), 164–181.

Cinquegrana, A. (1989). The walls (and wires) have ears: The background and first ten years of the Foreign Intelligence Surveillance Act of 1978. *University of Pennsylvania Law Review*, *137*(3), 793–828.

Clement, A., McCann, C., Resch, G., & Stewart, E. (2012, February). *IXMaps: Tracking your information packets over the net, through exchange points and across borders.* Paper presented at iConference: Culture, design, society, University of Toronto, Toronto, Ontario.

Cohn, C., & Timm, T. (2013, December 26). 2013 in review: The year the NSA finally admitted its "collect it all" strategy. *Electronic Frontier Foundation.* Retrieved from https://www.eff.org/deeplinks/2013/12/2013-year-nsas-collect-it-all-strategy-was-revealed

Collins, P. H. (2005). *Black sexual politics: African Americans, gender, and the new racism*. New York, NY: Routledge.

Drucker, J., & Nowviskie, B. (2004). Speculative computing: Aesthetic provocations in humanities computing. In S. Schreibman, R. Siemens, & J. Unsworth (Eds.), *A companion to digital humanities* (pp. 431–447)*.* Oxford, UK: Blackwell.

Forgang, J. (2009). Right of the people: The NSA, the FISA Amendments Act of 2008, and foreign intelligence surveillance of Americans overseas. *Fordham Law Review*, *78*(1), 217–266.

Funk, W. (2007). Electronic surveillance of terrorism: The intelligence/law enforcement dilemma—A history. *Lewis & Clark Law Review*, *11*(4), 1099–1140.

Gellman, B., & Poitras, L. (2013, June 6). U.S., British intelligence mining data from nine U.S. Internet

companies in broad secret program. *The Washington Post.* Retrieved from http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Greenwald, G. (2013, July 31). XKeyscore: NSA tool collects "nearly everything a user does on the Internet." *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Greenwald, G., & Ackerman, S. (2013, June 27). NSA collected U.S. email records in bulk for more than two years under Obama. *The Guardian.* Retrieved from http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama

Greenwald, G., Kaz, R., & Casado, J. (2013, July 6). UA espionaram milhões de e-mails e ligações de brasileiros [United States spied on millions of e-mails and calls from Brazil]. *O Globo.* Retrieved from http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934

Hallinan, B. & Striphas, T. (2016). Recommended for you: The Netflix Prize and the production of algorithmic culture. *New Media & Society*, *18*(1), 117–137.

Henriques, H. S. Q., & Schuster, E. J. (1917). "Jus soli" or "jus sanguinis"? *Problems of the War*, *3*, 119–131.

Holder, E. (2009a). Exhibit A: Procedures used by the National Security Agency for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended. Retrieved from http://www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document

Holder, E. (2009b). Exhibit B: Procedures used by the National Security Agency for targeting non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended. Retrieved from http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document

Kerr, O. S. (2011). An equilibrium-adjustment theory of the Fourth Amendment. *Harvard Law Review*, *125*(2), 476–543.

Lingel, J., & Golub, A. (2015). In face on Facebook: Brooklyn's drag community and sociotechnical practices of online communication. *Journal of Computer-Mediated Communication*, *20*, 536–553.

Maclin, T. (1998). Race and the Fourth Amendment. *Vanderbilt Law Review*, *51*(2), 331–394.

Manovich, L. (2001). *Language of new media*. Cambridge, MA: MIT Press.

Mascolo, E. (1972). The emergency doctrine exception to the warrant requirement under the Fourth Amendment. *Buffalo Law Review*, *22*, 419–438.

May, S. (2001). *Language and minority rights: Ethnicity, nationalism, and the politics of language*. New York, NY: Routledge.

Nakashima, E., & Warrick, J. (2013, July 14). For NSA chief, terrorist threat drives passion to "collect it all." *The Washington Post.* Retrieved from https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html

National Security Agency. (2013). NSA PRISM program slides. *The Guardian.* Retrieved from http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document

National Security Agency. (2014). *New collection posture.* Retrieved from https:// www.aclu.org/files/natsec/nsa/20140722/New%20Data%20Collection %20Posture.pdf

Ngai, M. (2014). *Impossible subjects: Illegal aliens and the making of modern America*. Princeton, NJ: Princeton University Press.

Norddeutscher Rundfunk. (2014, January 26). Snowden-interview: Transcript. Retrieved from http://www.ndr.de/nachrichten/netzwelt/snowden277_page-3.html

Pasquale, F. (2015). *The black box society: The secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Rose, N. (2009). *The politics of life itself: Biomedicine, power, and subjectivity in the twenty-first century*. Princeton, NJ: Princeton University Press.

Rouvroy, A. (2013). The end(s) of critique: Data behaviorism versus due process. In M. Hildebrandt & K. de Vries (Eds.), *Privacy, due process, and the computational turn: The philosophy of law meets the philosophy of technology* (pp. 143–168). New York, NY: Routledge.

Singel, R. (2006, April 7). Whistle-blower outs NSA spy room. *Wired.* Retrieved from http://archive.wired.com/science/discoveries/news/2006/04/70619

Sullivan, J. (2014). From the purpose to a significant purpose: Assessing the constitutionality of the Foreign Intelligence Surveillance Act under the Fourth Amendment. *Notre Dame Journal of Law, Ethics & Public Policy*, *19*(1), 379–413.

Timberg, C. (2013, July 10). NSA slide shows surveillance of undersea cables. *The Washington Post.* Retrieved from http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html

Torpey, J. (2000). *The invention of the passport: Surveillance, citizenship and the state*. Cambridge, UK: Cambridge University Press.

USA PATRIOT ACT, H.R. 3162, 107th Cong. (2001). Retrieved from http://www.fincen.gov/hr3162.pdf

Whitehead, J., & Aden, S. (2002). Forfeiting "Enduring Freedom" for "Homeland Security": A constitutional analysis of the USA Patriot Act and the Justice Department's anti-terrorism initiatives. *American University Law Review*, *51*(6), 1081–1133.

Wong, E. L. (2015). *Racial reconstruction: Black inclusion, Chinese exclusion, and the fictions of citizenship*. New York, NY: New York University Press.