GeoJournal
DOI 10.1007/s10708-014-9598-y

Collect it all: national security, Big Data and governance

Jeremy W. Crampton

Abstract This paper is a case study of complications of Big Data. The case study draws from the US intelligence community, but the issues are applicable on a wide scale to Big Data. There are two ways Big Data are making a big impact: a reconceptualization of (geo)privacy, and "algorithmic security." Geoprivacy is revealed as a geopolitical assemblage rather than something possessed and is part of emerging political economy of technology and neoliberal markets. Security has become increasingly algorithmic and biometric, enrolling Big Data to disambiguate the biopolitical subject. Geoweb and remote sensing technologies, companies, and knowledges are imbricated in this assemblage of algorithmic security. I conclude with three spaces of intervention; new critical histories of the geoweb that trace the relationship of geography and the state; a fuller political economy of the geoweb and its circulations of geographical knowledge; and legislative and encryption efforts that enable the geographic community to participate in public debate.

Keywords Big Data · Privacy · National security · Geoweb · Political economy

J. W. Crampton (✉)
Department of Geography, University of Kentucky, Lexington, KY 40506, USA
e-mail: jcrampton@uky.edu

> "Collect it all, process it all, exploit it all, sniff it all, know it all." NSA Collection Posture revealed in Snowden documents (Greenwald 2014, 97).

This paper is a case study of complications that attend Big Data. The case study is drawn from the world of the US intelligence community (IC) as it pertains to national security, but the issues raised are applicable on a wide scale to Big Data.

The case study reveals two critical issues where Big Data is making a big impact: a reconceptualization of privacy, especially geolocational privacy, and what may be called "algorithmic security." Geoprivacy is revealed as a geopolitical assemblage rather than an entity which is possessed (Dittmer 2014; Elwood and Leszczynski 2011) and is part of an emerging political economy of technology and neoliberal markets described by Leszczynski (2012). These assemblages are more than discursive, they are also material and maintain relations of exteriority such that "component parts of a whole cannot be reduced to their function within that whole" (Dittmer 2014, 387). Rather than the state retreating or "rolling back" from geospatial governance, I contend there is no clear distinction between the strategic and economic. This point is best evidenced through security and its algorithmic and biometric practices (Amoore 2009). As I have argued elsewhere, the state is spinning off and extending its capabilities, especially in the defense and intelligence sectors (Crampton 2012; Crampton et al. 2014).

Published online: 11 October 2014

Geoweb and remote sensing technologies, companies, and knowledges are imbricated in this assemblage of algorithmic security. As we shall see later in this paper, geopolitical assemblages are also actively engaged in various codings and decodings, particularly around the algorithmic subject. The Snowden documents have taught us that security and privacy must be thought together, not as trade-offs as is usually the case, but as mutually constituting.

There are attractive reasons for choosing the IC to discuss Big Data. First, the US IC is a big, complex and multifaceted enterprise that touches the lives of millions of Americans and non-Americans. With an annual budget which peaked at $80 billion in FY 2010, there are 16 IC agencies, including the National Security Agency (NSA) and the National Geospatial-Intelligence Agency (NGS) which performs remote sensing and geographic analysis, and is consequently of much relevance to geographers.

Second, the IC does not just comprise government, but also enrolls academia, social media such as Twitter, Google, Facebook, and has extensive contracts with private companies (including GIS companies such as Esri). As such, it reaches into many aspects of life in the US and around the world that Big Data researchers are interested in, especially what is known in the IC as "human dynamics" or how humans move, interact, behave and the models and understandings that emerge from the study, often known as activity based intelligence (ABI).

Third, the IC and Department of Defense are avid producers and consumers of Big Data. The NSA alone captures and analyzes the "full take" (the content of every single phone call) of at least two countries around the world, the Bahamas, and "country X"[1] amounting to billions of data which can be stored and searched for up to 30 days (Devereaux et al. 2014). One NSA capability known as SHELLTRUMPET processed its one trillionth record in December 2012 (Greenwald 2014). "Bulk" surveillance is also carried out within the USA; intercepting, storing and analyzing the metadata of millions of Americans' phone calls. As one defense contractor put it, Big Data offers the potential of "limitless intelligence" (Sorenson 2013).

Finally, the IC has since June 2013 received massive attention, public debate and reform efforts due to the documents provided by former NSA contractor Edward J. Snowden. President Obama in a press conference in August 2013 indicated he favored a "vigorous public debate" about the implications of intelligence practices (e.g., on privacy).[2] These public debates have focused much attention on intelligence surveillance and Big Data. In May 2014 the White House issued a major report on Big Data and privacy by a working group led by the President's Counselor John Podesta.[3] As others have recognized, the Snowden documents "offer a unique opportunity to grapple with Big Data surveillance" (Lyon 2014, 5). My paper is an intervention into these ongoing debates.

For the purposes of this paper I use a three-pronged definition of Big Data that tracks recent usage of the term:

> [F]irst, it refers to technology that maximizes computational power and algorithmic accuracy; second, it describes types of analysis that draw on a range of tools to clean and compare data, and third, it promotes a certain mythology – the belief that large data sets generate results with greater truth, objectivity, and accuracy (Crawford and Schultz 2013, 5).

In other words, Big Data are a matter of technologic *practices*; *epistemologies;* and *ontologies*.

Paradoxes of Big Data

Richards and King (2013) recently identified three paradoxes which lie at the heart of Big Data. Although they accept that Big Data can and does have beneficial outcomes, they argue that the evidence of these benefits has not been balanced with a look at the limits or undesirable outcomes of Big Data. First, Big Data suffer from a "transparency paradox." That is, whereas the "operations of big data itself are almost entirely shrouded in legal and commercial secrecy" (2013, 42) those same operations have, in the words of one recently leaked NSA document "peeled back the

[1] Wikileaks identified country X as Afghanistan (http://bit.ly/1niGf56).

[2] See http://wh.gov/lg4h2.

[3] See http://1.usa.gov/1f4w8re.

onion" of personal and collective privacy (Ball et al. 2013).

Second, Big Data creates an "identity paradox." Whereas individuals seek control over the formation of their identity, Big Data constitutes identity. In spatial terms identity formation may occur when an individual's geolocational information is surveilled and analyzed in "biopolitical spatial profiling" (Crampton 2007). Several authors have proposed variants of a "decentered" understanding of privacy/surveillance/data; for example Amoore's "data derivatives" (Amoore 2011) and Cohen's notion of a "modulated democracy" of pervasive surveillance that attempts to fix and predict (and hence construct) the subject (Cohen 2012b). More generally, we can see that the same concept is described by Foucault as indicative of the political rationality of the modern state that simultaneously individualizes and forms populations—or biopolitical governance (Foucault 2000). In the intelligence world, Big Data is central to the development of "human dynamics," otherwise known as ABI and "patterns of life" analysis.

Third, Richards and King identify a "power paradox." Big Data are a powerful tool that will "revolutionize" our lives (Mayer-Schönberger and Cukier 2013), yet Big Data sensors, tools and applications are in the hands of powerful institutions rather than ordinary people. Big Data may therefore be exacerbating inequalities and exploitation, rather than ameliorating them. "Privacy information markets" arise where privacy becomes a market commodity that can be bought (e.g., a premium version of an app without tracking ads) or sold. The purpose of these markets is not to increase the supply of privacy, but rather the opposite (Cohen 2012a). Privacy can be "extracted" as surplus value (Harvey's "accumulation by dispossession") by social media technologies, in return for a (disproportionately low) benefit to the user, for example the social capital gained from being on Facebook (Ellison et al. 2007). This argument harks back to the classic observation of the "factory in the livingroom" by Jhally and Livant (1986) that watching television is an instance of producing value (that is, working) by paying attention to advertisements. In turn, this attention can be sold on. If this is correct, we might ask if geolocational tagging (whether deliberately or as part of our data exhaust) is similarly a form of the production of surplus value? If so, this would have huge implications for geoweb studies, as the object of study would not necessarily be the content of geotagged information (e.g., maps of Tweets and geographies of the Internet) but for example how subjects are constituted as laborers in an exploitive economic system. On this view (paying attention to what people do under neoliberalism rather than the content of their online activities), there is a huge power imbalance (asymmetry) in socio-economic terms regarding Big Data. Schneier calls this "surveillance as business model."[4]

In the next section of the paper, I look at these three paradoxes or complications that attend Big Data. I show that the practices of the intelligence community highlight the work that Big Data does. In particular, it illustrates several of the principles of "critical data studies" (boyd and Crawford 2012; Dalton and Thatcher 2014). Despite the push-back against Big Data as being less effectual than its grandiose claims (e.g., Anderson 2008), the forgetfulness of its own history (Barnes 2014), and the need to avoid reifying it, Big Data has nevertheless been part of two key questions that are explicitly evidenced by the intelligence community: reconceptualizations of privacy as geopolitical assemblage, and "algorithmic security."

Privacy as geopolitical assemblage

In a recent paper Elwood and Leszczynski (2011) focus less on defining what privacy "is" and more on societal struggles over it. One such struggle that has been going on for several decades is that between privacy and surveillance (especially by the state). Much of this surveillance is performed by America's national intelligence agencies. These had their origins in World War II, including what would become the NSA, the National Geospatial-Intelligence Agency (NGA) and the National Reconnaissance Office (NRO) responsible for surveillance satellites. The Snowden documents and historical research on specific agencies such as the NSA, the OSS and the NGA have clarified the scope and practices of the intelligence community (Bamford 1982, 2008; Barnes 2006; Richelson 1995, 2012).

The secret world grew rapidly after September 11, 2001 (9/11). Several official indicators are available to

[4] See https://www.schneier.com/blog/archives/2013/11/surveillance_as_1.html.

measure its size. After Congress mandated that the number of persons with security clearances be published, in 2014 it was disclosed that there were 4,917,751 people with security clearances. This number includes some 1.4 m people with the highest security clearance, Top Secret, and at least 1 m contractors with clearances.[5] The nearly 5 m cleared personnel represents an increase of about 1.1 % over the previous year.

According to the Snowden documents, there are 107,035 "core" employees of the intelligence community (7.6 % of all Top Secret-cleared personnel). Core employees are those that perform essential government activities such as imagery analysis that cannot be contracted out. The Snowden documents reveal there are about 8,500 people working in the National Geospatial-Intelligence Program (NGP)—the remote sensing imagery, GIS, and geographic intelligence (GEOINT) effort of the US government—which consumes about 9 % of the intelligence budget or $4.7B (Gellman and Miller 2013). However, there is a huge penumbra of intelligence contractors, non-cleared personnel, and others from whom the government receives intelligence products and services. In this context it should be remembered that Snowden was a former CIA and NSA contractor, not a government employee.

In recent years the top-line budget on IC funding has also been disclosed. The IC budget grew every year after 9/11, and reached a peak in 2010 of $80.1B. Budgets have since then ranged between $65-70B; still far above pre-9/11 levels.

Yet much remains hidden. The Obama administration has often acted to curtail public knowledge of its intelligence and surveillance activities, particularly against whistleblowers. While it has passed whistleblower protections for people with access to classified information (i.e., the IC) in order to report waste, fraud and abuse (Presidential Policy Directive 19, known as PPD-19),[6] the PPD specifically precludes a leak to the press as a protected act of whistleblowing (even where it reveals fraud, waste or abuse). Furthermore, in 2014 the Director of National Intelligence (DNI), James Clapper, issued a directive requiring IC members and contractors to obtain pre-publication clearance before speaking to the press, even if the information is unclassified.[7]

The Obama administration has additionally prosecuted individuals from the IC who have leaked information, even where that information is not classified. It has brought eight such leak cases (compared to three in all previous administrations). These cases have received extensive media attention because the Obama administration has reached back to the 1917 Espionage Act to file espionage charges, for example against Manning (sentenced to 35 years) and Edward Snowden (currently an asylee in Russia) thus putting them in the same category as spies or foreign agents.

These three actions (curtailing the definition of whistleblowing, requiring pre-clearance, and expanded legal definitions) underline the efforts the US government makes to ensure the asymmetric balance of information is continued. These changes to the legal system are exemplars of what Wendy Brown calls "tweaks" that enable neoliberal government to "undo" democracy (Brown 2014). Although small in nature, they have magnified political effects and constitute a vital part of the geopolitical assemblage.

No discussion of government surveillance or Big Data can now take place without reference to the ongoing publication of the documents released by former NSA contractor Edward Snowden (Lyon 2014). These documents are of course part of the reason for the regulative tweaks against what the IC calls "insider threats." However, although they do provide perhaps the single largest insight into Big Data surveillance, they are mostly limited to one agency (NSA), and need careful interpretation and historical perspective. Much more is still required about the activities of other agencies (especially the FBI and the NGA) and contractors. Nevertheless, the documents raise important questions about geoprivacy, surveillance and the state.

The first revelations, in June 2013, concerned two broad NSA intelligence efforts: telephony and Internet traffic. These efforts are authorized as part of the NSA's mission by at least four legal statutes; Executive Order 12333 of 1981 (as amended in 2004 and 2008), the 1978 Foreign Intelligence Surveillance Act

[5] The government was unable to determine if about 300,000 cleared individuals were government employees or contractors, so 1 m contractors is likely to be a lower bound.

[6] http://www.fas.org/irp/offdocs/ppd/ppd-19.pdf.

[7] See http://blogs.fas.org/secrecy/2014/05/odni-prepub/.

(FISA), Section W702 of the 2008 FISA Amendments Act (FAA), and Section 215 of the 2001 Patriot Act. Accordingly the NSA stipulates that all its activities are legal (that is, covered by legal authorities)—although they are by no means uncontroversial even within the IC (Clarke 2004; Mayer 2008). These authorities have been legally contested, and some of the legal interpretations of authority are still secret (so-called "secret laws"). An example of the latter is how the FISA Court secretly reinterpreted the law (Section 215 of the Patriot Act) to allow bulk surveillance of US telecoms in 2006 (Gellman 2013). Among others, the ACLU has filed suit against these practices as being unconstitutional.

The first Snowden document released was a Top Secret warrant from the Foreign Intelligence Surveillance Court (FISC) dated April 25, 2013 (Greenwald 2013). The warrant directed that Verizon, one of America's largest telecom companies, turn over the "daily, ongoing" records of potentially millions of Americans, including solely local calls. (Other companies such as AT&T and Bell South also provide records.) The FISC order covers bulk collection of cell phone metadata of US persons. Because metadata is deemed to be in the public sphere (and indeed is needed by telecoms to route calls) it has received lesser privacy protection than phone call content. President Obama has used this fact to assert that the government is not listening to Americans' phone calls and only collects metadata.

The FISA warrant does not explicitly mention geolocational tracking. Therefore, there are open questions how and to what extent such tracking is performed by the IC, and whether on an individual basis or in bulk. General Keith Alexander testified in Congress that although the NSA has the operational capacity to track cell phones, they do not do so currently (under Section 215). Geolocation has recently become a major topic of debate in legislative and government circles. Congressional hearings in April 2013 widely discussed the effects of requiring probable cause for geolocational tracking (113th Congress 2013) without resolving the issue. Senator Wyden (D-OR), a member of the Senate Intelligence Committee, has long pushed for cell phone tracking privacy legislation (known as the GPS Act) and has repeatedly indicated that Alexander and DNI James Clapper have not answered the question whether the government has ever collected, or ever planned to collect, geolocational data. Recent legal rulings by the Supreme Court (*US v. Jones* and *Riley v. California*) have provided an uncertain legal landscape for privacy; appearing to afford some protections without grounding them in a full right to geolocational privacy.

Since warrants can and have been interpreted to mean bulk surveillance, additional safeguards are required. For example, "cell tower dumps," which provide the data of all individuals at a location, could conceivably be covered by a warrant and thus subject to surveillance. The GPS Act makes some attempts to prohibit this. The law makes it illegal to acquire and provide services using geolocation data originating from wireless devices (it specifically mentions mapping) unless a warrant has been obtained. Exceptions provided by the law allow geolocation tracking by the telecom itself as part of its business, or as covered by FISA, or if the information is "public" or by "consent." But how are "consent" and "public information" to be interpreted? It is possible that consent may be implied by the use of the device (or its terms of service), or by turning on location services in the device or app. There has been some question about this in light of the secretive study performed by Facebook on about 700,000 of its own users, since the platform's Terms of Service are so long as to possibly violate Institutional Review Board (IRB) protocols (Kramer et al. 2014). But it is likely that if you take a geotagged photograph or Tweet then this constitutes public consensually shared information (and thus studies mapping people's Tweets are legal).

The limitations of individually-targeted warrants are illustrated with newer geolocation capabilities revealed in the Snowden documents. In particular, what the NSA calls "co-traveler analytics" allows surveillance to acquire additional targets when individuals' cell phones "travel together." The key here is that the second (or third, or fourth, etc.) person was not previously a suspect and is not named in a warrant. However, their spatial behavior renders them a surveillance target; as many as five billion records a day according to the Snowden documents (Soltani and Gellman 2013).

For example, a program called CHALKFUN derives the time and place of a cell phone, then looks for other cell phones that were nearby within a 1-h time window. Another program, the DSD Co-Travel Analytic, can then spatially predict probable travel routes to determine if suspect and co-traveler will intersect locations. According to the NSA:

> (S//SI/REL TO USA, FVEY) This analytic was tested using an [REDACTED] terrorist case study. The case study used approximately 80,000 base stations locations and 16 billion mobiles location records for CDRs (Call detail records) and infrastructure collect from DRT [digital receiver technology] and Juggernaut [data ingest processing] systems. This case study showed that more candidate co-travellers were discovered by analyzing the travel paths than by considering common meeting locations alone.

Another program, HAPPYFOOT, intercepts mobile apps as they communicate with advertising networks. "Cookies" placed on phones by advertisers uniquely identify a browser, and the NSA will piggyback on these identifiers to track down and "exploit" the target device (i.e., to hack it) (Soltani et al. 2013). Outside the IC, cookies also represent a significant vector of attack that can be used to track users even without client-side identifiers (Nikiforakis et al. 2013). As Soltani et al. (2013) indicate:

> Apps transmit their locations to Google and other Internet companies because ads tied to a precise physical location can be more lucrative than generic ads. But in the process, they appear to tip off the NSA to a mobile device's precise physical location.

Another tracking possibility exploits the smartphone accelerometer. According to recent research, manufacturing imperfections in these devices, which track three-dimensional movements of the phone, enable them to be uniquely identified with 96 % accuracy. Accelerometer data signals used in apps could then be used to disambiguate and uniquely identify and track the phone without needing to know the phone number, the ICC-ID (SIM card number) or IMEI device ID (Dey et al. 2014). These researchers have also apparently solved the problem of knowing in which direction a smartphone is travelling, regardless of its orientation and movement (e.g., swinging around in a pocket), if the compass is not active (e.g., inside buildings) or a lack of WiFi (Roy et al. 2014)—a total biometrics of movement. Coupled together, these two features represent powerful geolocational tracking potential that may not require a warrant.

Perhaps the most surprising element of the geopolitical assemblage revealed in the Snowden documents has been the scope of the public–private cooperation of government and Internet companies.

The most significant of these is the PRISM program (Gellman and Poitras 2013) which works with the cooperation of nine prominent Internet developers of the geoweb, including Apple, Google, Yahoo and Microsoft. Among other capabilities, the NSA collects individuals' social media address books in the MAINWAY program (Risen and Poitras 2013) by the agency's Special Source Operations (SSO) branch (Gellman and Soltani 2013). According to SSO documents, a typical daily "intake" of email address books amounts to more than 250 million per year. In the MARINA program the NSA stores millions of users' Internet metadata for up to a year, even where those persons are not suspects in any investigation (Ball 2013). The everyday nature of information acquired and stored by the NSA is often highly intimate, including baby pictures, mental health crises, and love letters by people who were not suspects, but collected and stored from emails and instant messages nevertheless (Gellman et al. 2014).

The XKEYSCORE program is one of the NSA's largest capabilities for monitoring online activities, according to the Snowden documents. Snowden himself has claimed that it enables the user to read any email, Google search, chat session or website visited. The documents indicate that it is used to build a unique profile or fingerprint of a user. One NSA slide shows that it tracks online mapping activities (Greenwald 2014). Other Snowden documents appear to show the NSA surveils US persons within the United States, including a former Republican candidate for office, apparently using FISA warrants, who are not terrorist suspects but are Muslims (Greenwald and Hussain 2014). Furthermore, the ratio of "incidental" collection (predictable but inadvertent collection) and retention of that information (even *after* minimization by hand by NSA analysts) to actual targets is at least 9 to 1 (Gellman et al. 2014).[8]

The "Upstream" program taps directly into the fiber optic "backbone" of the Internet. If PRISM is the legally compelled front door, Upstream is the back door. One of the more remarkable government sources of data, which includes data on Americans, is the MUSCULAR program, which operates with the UK's

[8] According to Gellman et al. (2014) a "target" may indicate a single individual or an IP address used by hundreds of persons.

GCHQ. It accesses the fiber-optic cables that connect the data centers of Facebook, Google and others, and apparently can remove SSL protections (Gellman and Soltani 2013b). Documents show several of the Silicon Valley companies actually made it easier for the government to obtain data, especially Microsoft and its SkyDrive, Skype and Outlook.com services (Greenwald 2014). These issues are very sensitive to the companies, because they see themselves as competing on privacy; that is, a key source of added value to their product is the personal privacy protection it supposedly offers. The documents appear to tell a very different story about privacy and geolocational tracking.

When these corporate connections to surveillance programs were revealed the companies expressed a series of denials or harm minimization statements (e.g., Google said it would begin encrypting Gmail). In effect, however, the government uses these companies to collect data on millions of individuals rather than acquiring it directly from those individuals. The result is a "government-corporate surveillance partnership" in the words of security expert Bruce Schneier.[9]

Companies ranging from Silicon Valley giants such as Google to smaller start-ups are in the same market as government when it comes to geospatial data and services. For example, both government and geoweb companies require tremendous quantities of imagery and enter into mutual agreements in large financial deals. This does not just entail government purchasing of commercial remote sensing imagery, but government underwriting of research, testing and the launch of corporate satellites to the tune of $7.3B for DigitalGlobe (Crampton et al. 2014).[10] In 2014 Google acquired the drone company Titan Aerospace, and also acquired satellite start-up Skybox for $500 M following the successful launch of a planned series of satellites (Barr et al. 2014).[11] This company is especially notable in that it partners with geoweb startup Mapbox/Tilemill and attended the most recent GEOINT conference in April 2014. (Its CEO has aerospace industry experience at the McDonnell Douglas (now Boeing) "Phantom Works" which was started to compete with the famous "Skunk Works" at Lockheed Martin that built advanced military equipment.) Since April 2014 Mapbox has also partnered with DigitalGlobe to bring imagery to OpenStreetMap (OSM). The partnerships, capital flows and investments of these companies is as yet little studied.

Following from the developments noted above, I argue that there is a critical need to develop a theory of the political economy of the geoweb, or more formally the spatialized information economy. Such a theory would have to accommodate finance and capital investment, and the underwriting of research by the DoD (e.g., DARPA and NGA grants), as well as histories of geoweb companies such as Mapbox and Geocommons, and the development of the GIS project at Harvard University in the 1960s (Wilson Forthcoming). Leszczynski (2012) has argued that the geoweb is part of a political economic transition that marks a significant roll-back of government involvement in the geoweb. For her, "markedly non-state (market and corporate) regimes of spatial data governance are rolling out in its place" (2012, 73). Although I agree that there has been a restructuring under neoliberal capital of the geoweb, and that Leszczynski is sensitive to the continued role of the state, I argue that market and corporate activities actively *extend* the state by increasing its reliance on the private sector (Crampton 2012).

Algorithmic security

Any theoretical understanding of the geoweb must address the formation of new political subjectivities, or what Cohen has called the "networked self" (Cohen 2012b) and Schwartz and Halegoua (2014) call "the spatial self." In the second part of the paper I discuss how information derived from sensors illustrates the identity and power paradoxes of Big Data. The main topics addressed here are a form of intelligence known as ABI and the US secret drone warfare program (Gregory 2014).

The current US drone program began before 9/11 and is an extension of research into robotics (Singer

[9] See http://bit.ly/1nUKoYV.

[10] The contract was signed in 2010 but has since been complicated by government sequestration and cut-backs, and the merging of DigitalGlobe and GeoEye in early 2013. The contract provided government funds for WorldView-3, DigitalGlobe's 0.31 m resolution satellite launched in August 2014. Six months after launch, DigitalGlobe will be permitted to sell panchromatic imagery up to 0.25 m.

[11] One geopolitical complication is that the launches take place in Baikonur Cosmodrome, which is Russian-controlled. US sanctions against Russia may prohibit future launches.

2009). They were initially used in the Balkan wars of the mid-1990s, primarily for reconnaissance. The first acknowledgement by the administration of its drone usage came in April 2012, when John O. Brennan, then counterterrorism advisor to President Obama (and now CIA Director), discussed them in a speech at the Wilson Center (Miller 2012a).

In a major speech in May 2013, President Obama spoke of the need to pursue "persistent, targeted efforts" to strike at terrorist networks beyond Afghanistan with RPAs or drones. He stated that they were effective, covered by Congressional Authorization for Use of Military Force (AUMF) as codified in law as 115 Statute 224, and were subject to clear oversight and accountability through a new Presidential Policy Guidance (PPG) document. The PPG stated a preference for capture, and that the US must have "near certainty" knowledge that the terrorist is present at the location, that non-combatants will not be injured or killed, and that capture is not feasible. The PPG did not rule out strikes against US persons, although it said that it would conduct an extra "legal analysis" to make sure the action was consistent with law–without, however, promising to release that analysis. To make these decisions, the government would "be informed by a broad analysis of an intended target's current and past role in plots…[and] relevant intelligence information the individual could provide" (U.S. Government 2013, 3).

The meaning of these phrases has become clearer with additional reporting in the press and information from the Snowden documents. Perhaps the most evocative is the so-called "disposition matrix," a database on terrorist threats (Miller 2012b). According to press reports based on interviews with national security officials, the matrix goes beyond previous kill/capture lists to include targets beyond the reach of drones.

But it is not only the offensive capability of drones that is concerning, but their use as sources of information that algorithmically piece together Amoore's "data derivatives" on human behavior and the environment (such as automated feature extraction from imagery) into actionable databases (Amoore 2014). As Amoore suggests "[w]hat is sought…[is] a *potential* terrorist, a subject who is not yet fully in view, who may be unnamed and as yet unrecognizable" (Amoore 2014, 109). Building big databases for national security purposes of behavior, movement, networks of contacts, remote sensing intelligence and GEOINT is not new. Precursors include the "human terrain" program built in Iraq during the 2000s and more recently used in Afghanistan, which in turn was based on the concept of counterinsurgency (COIN). What makes COIN different from regular "kinetic" warfare is that it pipes in knowledge (data) on a host of cultural and other variables in order to distinguish the "right" people to kill. As Gregory has argued, it is the military's version of the "cultural turn" (Gregory 2008).

A driver of ABI is that according to the DoD, COIN and Intelligence, Surveillance and Reconnaissance (ISR) operations were suffering from inadequate "social and behavioral science data, including human geography" while at the same time they were drowning in sensor information (Defense Science Board Task Force on Defense Intelligence 2011, 62). ISR refers to the technical collection of intelligence from airborne platforms (including drones and satellites). The Board recommended much more intensive research in the "computational social sciences and social network analysis," behavioral modeling and simulation, human terrain data collection, and biometrics. The purpose is to provide a renewed focus on "population security, governance, and economic development" (2011, 7). The report identified specific disciplines that could contribute to the identification of causal factors of insurgency, including economic crises, climate change, demographic pressures, poor governance and resource scarcity. Anthropology and sociology, human and cultural geography were all identified as sources of ISR. This would be achieved by identifying "key indicators" and the development of "activity norms" (2011, 18) and "target signatures" ("organizational structure, communications, movement" (2011, 28).

Concrete definitions of ABI are notoriously scarce, but it can be thought of as (big) databases to identify and isolate specific patterns of activity rather than simply surveilling areas of interest. It is an approach to address the problem of the surfeit of data.[12] Roughly, if surveillance is image-based, we may say that ABI is object-based. Instead of surveilling known targets, it is a form of data-mining that identifies the anomalous signatures the DoD ISR report requested. Although

[12] One company, DigitalGlobe, has approximately 50 petabytes of data.

both drones and satellites can be used to acquire imagery, drones have the advantage of persistence; to "dwell" over an area where a satellite has to continuously move along its orbit. Drones are also much closer to the ground (i.e., below cloud cover).

Attention to ABI is expanding across the IC. It formed one of the main themes of the 2013 GEOINT Conference. The NGA recently awarded a $60 million contract to BAE to develop ABI products that could exploit the same types of metadata revealed in the Snowden documents (Miller 2013). According to the Director of the NGA, Letitia Long, ABI can "identify patterns, trends, networks and relationships hidden within large data collections" (Miller 2013). ABI is particularly good at geolocational data since all "events" (activities of interest, not just of the target but of all the connections and networks connecting to the target) can be geotagged and mapped.

Speaking in 1979 Foucault already gave a very good account of the purpose of efforts such as ABI:

> men and their things are envisioned as to their relationships: men's coexistence on a territory; their relationships as to property; what they produce; what is exchanged on the market. It also considers how they live, the diseases and accidents that can befall them. What the police sees to is a live, active, productive man (Foucault 2000, 319).

Foucault calls this an "art of government" or governmentality that was simultaneously individualizaing and totalizing.

Telephony and online intelligence continues to play a role here too. Perhaps of most interest are the geolocational capabilities of co-traveler analytics discussed above and their algorithmic abilities. NSA's CHALKFUN program for example is described as:

> (TS//SI/REL TO USA, FVEY) Chalkfun's Co-Travel analytic computes the date, time, and network location of a mobile phone over a given time period, and then looks for other mobile phones that were seen in the same network locations around a one hour time window. When a selector was seen at the same location (e.g., VLR [visitor location register]) during the time window, the algorithm will reduce processing time by choosing a few events to match over the time period. Chalkfun is SPCMA enabled.
>
> (S//SI//REL) SPCMA enables the analytic to chain "from," "through," or "to" communications metadata fields without regard to the nationality or location of the communicants, and users may view those same communications metadata fields in an unmasked form.

The significance of this is that it allows the NSA or other agencies to search the database without specifying a target (a "selector"). Therefore an individual may be geolocationally tracked after being identified by the algorithm regardless of whether they had previously been identified as a target:

> location data, especially when aggregated over time, are widely regarded among privacy advocates as uniquely sensitive. Sophisticated mathematical techniques enable NSA analysts to map cellphone owners' relationships by correlating their patterns of movement over time with thousands or millions of other phone users who cross their paths. Cellphones broadcast their locations even when they are not being used to place a call or send a text message (Gellman and Soltani 2013c).

A series of white papers by the Undersecretary of Defense for Intelligence (USD(I)) point to the fact that "humans, unlike other entities, are inherently self-documenting" especially through social media such as Twitter, Facebook and LinkedIn (cited in Miller 2013). ABI is conceived as the geospatial fusion of multi-INT sources, meaning it draws from GEOINT, SIGINT, HUMINT and the other forms of intelligence (Murdock et al. 2014). Given the disparity of these data, the one field they have in common is location, notes the NGA (Quinn 2012). Long often mentions the need for the NGA to incorporate "human geography" into its mission as a combat-support agency (Alderton 2013).

Actions and reforms

To be secret means "to set apart, withdrawn, hidden" (L. *secretus*) in an act of separating. Privacy means to retain unto oneself (L. *privus*), a sense of "one's own." The classic formulation was given by justices Warren and Brandeis in 1890 as "the right to be let alone" (Warren and Brandeis 1890). Traditionally therefore

privacy is conceived as blending secrecy (anonymity) and autonomy of action outside the scope of external forces (to be let alone). This concept of privacy no longer seems adequate to today's context. Nor does it provide sufficient political purchase for opposition to inroads to privacy, especially if it means privacy is opposed to security in a zero-sum game.

If it is true that privacy is a geopolitical assemblage, as I have argued here, a commensurately wide-reaching set of responses seems called for. In conclusion then, let me suggest three points of action that will concretely act to reverse Big Data asymmetries and which may point a way to a critical theory of the political economy of the geoweb. These suggestions are preliminary; my reading of the geoweb literature on privacy is that it is longer on analysis than on action but that researchers are eager to engage.

First, we should address the secrecy of the security state; the huge amount of work done in secret under security clearances, the massive outsourcing, and over-classification. *We need better histories and contemporary accounts of the national intelligence community—especially regarding its geographical and mapping (including GIS) components: a genealogy of mapping.*

Second, perhaps the biggest single obstacle to knowing more about the security state is that so much of it is outsourced to private companies. These operate with even less transparency than the federal government. Therefore, we should make IC contracting more accountable: require reporting of the scope and capabilities of contracts, make the government bidding process more transparent, and open the "black budget" that is presented to Congress to the public. *We need a better understanding of the economies and capital flows of GEOINT and spatialized information.*

Third, we require better legal and encryption protections. Snowden's primary motivation, according to him, is for legal reform that provides the public with the ability to make an informed decision about government surveillance (akin to informed consent). Although new legislation has been introduced that curtails bulk surveillance (the USA Freedom Act, HR 3361) this has received a mixed reception and after initially supporting it, civil liberties groups reacted with skepticism to the bill passed in the House. Indeed, geolocation surveillance may have been expanded to codify co-traveler analytics described above.

One problem is that legislation is outdated in terms of today's capabilities. The major law covering communications privacy such as wiretaps (the Electronic Communications Privacy Act, ECPA) was passed in 1986. Technological advances mean that it is now so much cheaper to track people compared to traditional physical surveillance that it constitutes a different kind of surveillance (Bankston and Soltani 2014, 337).

A similar finding was expressed by a team investigating the "mosaic theory" of the Fourth Amendment in the context of surveillance. They found that current technology could stitch together or mosaic a sufficient degree of surveillance to constitute a constitutional violation after only a week, even if individually each data point did not (Bellovin et al. 2014).[13] This capability is expressly algorithmic, searching through database to find sufficient data derivatives to stitch together a surveillant pattern.

These understandings of privacy comport with the view advanced in this paper of a geopolitical assemblage to take into account a range of factors governing privacy (legal, technological, political). In effect there have been non-legal "rights" to privacy that are afforded in practice by physical and technological barriers that make surveillance cost-prohibitive (Surden 2007). When those barriers are removed, then privacy becomes less protected. Bankston and Soltani (2014) compared the cost of different location tracking capabilities and found that the cost of cellphone tracking was only 1/50th of traditional surveillance (a five-man "surveillance box" which surrounds the target on all sides).

A related necessary area of protection is encryption. If a user could practice end-to-end encryption it would hardly matter what surveillance capabilities were available.[14] Although there is surely a rich geography

[13] The Supreme Court case *United States v. Jones* has proved to be the most significant ruling to date. The justices ruled that a GPS tracker placed on a car without a warrant was unconstitutional (although violation of privacy was not determining).

[14] For example, Internet companies such as Google and Yahoo could practice encryption such as PGP. However, there are market and government forces strongly resisting such a development. For these companies the user is a "product" whose privacy is bought and sold on. Additionally, the companies are susceptible to a National Security Letter (NSL) which could secretly demand the master encryption key from the company. There is no recourse against a secret NSL, except ultimately to shut down the service, as the Lavabit email

of encryption exploits, zero-day vulnerabilities and virus and worm targets (such as the Heartbleed vulnerability), distributed denial of service (DDOS) and the global protections against them (such as encryption, cybersecurity, resilience to hacking, etc.), this is an area which as yet has received little attention. Cyberwarfare is no longer something that we can afford to ignore, especially given the prevalence of the Internet of Things and an estimated 50 billion Internet connected devices by the year 2020. If researchers have made progress theorizing the web (Leszczynski and Wilson 2013), then material and practical responses must also be configured. One way in which this may be done, is to build on the work on codes and algorithms (Amoore 2011; Mackenzie and Vurdubakis 2011) and critical theories of secrecy (Birchall 2011a, b).

Thus I recommend that geographical and geospatial organizations such as the Association of American Geographers (AAG), the American Society for Photogrammetry and Remote Sensing (ASPRS) and the United States Geographic Intelligence Foundation (USGIF) *should partner with civil rights organizations to actively pursue legislative reform for geoprivacy protections, including end-to-end encryption. Critical legal scholarship that is attentive to geolocational privacy is also worth expanding, particularly the intersections of law, space and power* (Blomley 1994; Braverman et al. 2014).

Conclusion

In this paper I have described contradictions and complications that lie at the heart of geospatial Big Data, as applied to one of its major instantiations, intelligence surveillance. It is a geopolitical assemblage that incorporates a nexus of interests including the state, the military, the legislature, the corporate world, and knowledge producers. None of these are easily separated from each other; indeed assemblage theory enables them to be examined collectively and to trace out the linkages and flows of cause and effect. Here I have drawn on Dittmer's recent conception of geopolitical assemblage to emphasize both discursive and material components of the geoweb, as well as its "relations of exteriority" which emphasize its irreducibility (Dittmer 2014, 387). For example, a solely technical or legal understanding would omit consideration of the biopolitics of life and subjectivities. If Foucault is correct that government both individualizes and totalizes, and if geospatial data, technologies and practices are all enrolled, then the critique of geoweb formations will require case studies that meet this complexity.

In this paper I have examined the intelligence community as such a case where we might gain perspective on these issues. Although more work needs to be done, it brings into view complications of Big Data in three specific registers: knowledge; identity (the algorithmic and biopolitical formation of subjects); and power.

In return, I have suggested three broad areas of response that I think are as yet still in their formative stages: critical histories of the geoweb (understood in Foucault's terms as genealogies that examine how subjects are constituted in regimes of truth); a political economy of the geoweb and how it is situated in a wider set of developments such as Big Data, smart cities, and everyday practices; and active legislative and practical/material efforts such as encryption that draw on the geographic community to operationalize a public debate that was brought into being so remarkably by Edward Snowden.

Footnote 14 continued
company did—an unlikely action for a Silicon Valley company. To the contrary, the Snowden documents show extensive private–public surveillance cooperation.

References

113th Congress, First Session. (2013). *Electronic Communications Privacy Act (ECPA) (Part II): Geolocation Privacy and Surveillance*. T. Subcommittee on Crime, Homeland Security and Investigations, of the Committee on the Judiciary. House of Representatives. Washington, DC: USGPO.

Alderton, M. (2013). Transformation within NGA promises new opportunities for the GEOINT community. *Trajectory Magazine, 3*. http://trajectorymagazine.com/web-exclusives/item/1552-geoint-30.html. Accessed October 20, 2013.

Amoore, L. (2009). Algorithmic war: Everyday geographies of the war on terror. *Antipode, 41*(1), 49–69.

Amoore, L. (2011). Data derivatives: On the emergence of a security risk calculus for our times. *Theory, Culture & Society, 28*(6), 24–43. doi:10.1177/0263276411417430.

Amoore, L. (2014). Security and the claim to privacy. *International Political Sociology, 8*(1), 108–112. doi:10.1111/ips.12044.

Anderson, C. (2008). The end of theory: The data deluge makes the scientific method obsolete. *Wired, 16*(7).

Ball, J., NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show. (2013, September 30). *The guardian*. http://gu.com/p/3j6mj/tw.

Ball, J., Schneier, B., & Greenwald, G., NSA and Gchq Target Tor Network That Protects Anonymity of Web Users. (2013, 4 October). *The guardian*. http://gu.com/p/3ja7d/tw. Accessed October 20, 2013.

Bamford, J. (1982). *The puzzle palace: A report on America's most secret agency*. Boston: Houghton Mifflin.

Bamford, J. (2008). *The shadow factory*. New York: Anchor Books.

Bankston, K. S., & Soltani, A. (2014). Tiny constables and the cost of surveillance: Making cents out of United States V. Jones. *The Yale Law Journal Online, 123*, 335–357.

Barnes, T. J. (2006). Geographical intelligence: American geographers and research and analysis in the office of strategic services 1941–1945. *Journal of Historical Geography, 32*, 149–168.

Barnes, T. J. (2014). Big Data, little history. *Dialogues in Human Geography, 3*(2), 297–302.

Barr, A., Winkler, R., & MacMillan, D., Google to Buy Satellite-Imaging Startup for $500 Million. (2014, June 10). *The Wall Street Journal*. http://online.wsj.com/articles/google-to-buy-satellite-imaging-company-for-500-million-1402421980. Accessed July 10, 2014.

Bellovin, S. M., Hutchins, R. M., Jabara, T., & Zimmeck, S. (2014). When enough is enough: Location tracking, mosaic theory, and machine learning. *New York University Journal of Law & Liberty, 8*(2), 555–628.

Birchall, C. (2011a). Introduction to 'secrecy and transparency': The politics of opacity and openness. *Theory, Culture & Society, 28*(7–8), 7–25.

Birchall, C. (2011b). Transparency, interrupted. Secrets of the Left. *Theory, Culture and Society, 28*(7–8), 60–84.

Blomley, N. K. (1994). *Law, space, and the geographies of power*. New York: Guilford Press.

Boyd, D., & Crawford, K. (2012). Critical questions for Big Data. *Information, Communication & Society, 15*(5), 662–679. doi:10.1080/1369118X.2012.678878.

Braverman, I., Blomley, N., Delaney, D., & Kedar, A. (2014). *The expanding spaces of law: A timely legal geography*. Stanford: Stanford University Press.

Brown, W. (2014). *Governmentality in the age of neoliberalism.* Paper presented at the Pacific Centre for Technology and Culture, University of Victoria, Canada.

Clarke, R. A. (2004). *Against all enemies: Inside America's war on terror*. New York: Free Press.

Cohen, J. E. (2012a). Irrational privacy? *Journal on Telecommunications and High Technology Law, 10*(2), 241–249.

Cohen, J. E. (2012b). *Configuring the networked self: Law, code, and the play of everyday practice*. New Haven: Yale University Press.

Crampton, J. W. (2007). The biopolitical justification for geosurveillance. *Geographical Review, 97*(3), 389–403.

Crampton, J. W. (2012). Outsourcing the state. *Geopolitics, 17*(3), 687–691.

Crampton, J. W., Roberts, S., & Poorthuis, A. (2014). The new political economy of geographic intelligence. *Annals of the Association of American Geographers, 104*(1), 196–214.

Crawford, K., & Schultz, J. (2013). Big Data and due process: Toward a framework to redress predictive privacy harms. *Boston College Law Review, 55*(1). Available at SSRN: http://ssrn.com/abstract=2325784.

Dalton, C., & Thatcher, J. (2014). What does a critical data studies look like, and why do we care? Seven points for a critical approach to 'Big Data.'. *Society and Space Open Site*. http://societyandspace.com/material/commentaries/craig-dalton-and-jim-thatcher-what-does-a-critical-data-studies-look-like-and-why-do-we-care-seven-points-for-a-critical-approach-to-big-data/. Accessed May 22, 2014.

Defense Science Board Task Force on Defense Intelligence. (2011). *Report of the defense science board task force on defense intelligence–Counterinsurgency (COIN) intelligence, surveillance, and reconnaissance (ISR) operations*. Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics.

Devereaux, R., Greenwald, G., & Poitras, L. (2014). Data pirates of the Caribbean: The NSA is recording every cell phone call in the Bahamas. (May 22). https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/. Accessed May 25, 2014.

Dey, S., Roy, N., Xu, W., Choudhury, R. R., & Nelakudit, S. (2014). *Accelprint: Imperfections of accelerometers make smartphones trackable.* Paper presented at the NDSS 14, San Diego, CA.

Dittmer, J. (2014). Geopolitical assemblages and complexity. *Progress in Human Geography, 38*(3), 385–401. doi:10.1177/0309132513501405.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of facebook "friends:" social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(4), 1143–1168. doi:10.1111/j.1083-6101.2007.00367.x.

Elwood, S., & Leszczynski, A. (2011). Privacy, reconsidered: New representations, data practices, and the geoweb. *Geoforum, 42*(1), 6–15.

Foucault, M. (2000). "Omnes Et Singulatim": Toward a critique of political reason. In J. Faubion (Ed.), *Power. The essential works of Michel Foucault 1954–1984.* (Vol. 3, pp. 298–325). New York: New Press.

Gellman, B., & Miller, G., US Spy Networks' Successes, Failures and Objectives Detailed in 'Black Budget' Summary. (2013, August 19). *The Washington Post*. Accessed May 25, 2014.

Gellman, B., & Poitras, L. US, British Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program. (2013, June 6). *The Washington Post*. http://wapo.st/1888aNq. Accessed October 17, 2013.

Gellman, B., & Soltani, A., NSA Collects Millions of E-Mail Address Books Globally. (2013a, October 14). *The Washington Post*. http://wapo.st/1gFM2f9. Accessed October 17, 2013.

Gellman, B., Tate, J., & Soltani, A. In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are. (2014, July 5). *The Washington Post*. http://wapo.st/1xyyGZF. Accessed July 10, 2014.

Gellman, B., US Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata. (2013, June 15). *The Washington Post*. http://wapo.st/JKDpDm. Accessed May 25, 2014.

Gellman, B., & Soltani, A., NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say. (2013b, October 30). *The Washington Post*. http://wapo.st/1dpsecg. Accessed May 25, 2014.

Gellman, B., & Soltani, A., NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show. (2013c, December 4, 2014). *The Washington Post*. http://wapo.st/IIaYWp. Accessed May 25, 2014.

Greenwald, G. (2014). *No place to hide*. New York: Metropolitan Books.

Greenwald, G., & Hussain, M., Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On. (2014). *The intercept*. https://firstlook.org/theintercept/article/2014/07/09/under-surveillance/. Accessed July 10, 2014.

Greenwald, G., NSA Collecting Phone Records of Millions of Verizon Customers Daily. (2013, June 6). *The guardian*. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. Accessed May 25, 2014.

Gregory, D. (2008). 'The rush to the intimate': Counterinsurgency and the cultural turn. *Radical Philosophy, 150*, 8–23.

Gregory, D. (2014). Drone geographies. *Radical Philosophy, 183*, 7–19.

Jhally, S., & Livant, B. (1986). Watching as working: The valorization of audience consciousness. *Journal of Communication*, *36*(3), 124–143.

Kramer, A. D. I., Guillory, J. E., & Hancock, J. T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences, 111*(24), 8788–8790. doi:10.1073/pnas.1320040111.

Leszczynski, A. (2012). Situating the geoweb in political economy. *Progress in Human Geography, 36*(1), 72–89.

Leszczynski, A., & Wilson, M. W. (2013). Guest editorial: Theorizing the geoweb. *GeoJournal, 78*(6), 915–919. doi:10.1007/s10708-013-9489-7.

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society, 1*(2), 1–13. doi:10.1177/2053951714541861.

Mackenzie, A., & Vurdubakis, T. (2011). Codes and codings in crisis: Signification, performativity and excess. *Theory, Culture & Society, 28*(6), 3–23. doi:10.1177/0263276411424761.

Mayer, J. (2008). *The dark side: The inside story of how the war on terror turned into a war on American ideals*. New York: Doubleday.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big Data: A revolution that will transform how we live, work, and think*. Boston: Houghton Mifflin Harcourt.

Miller, G., Activity-Based Intelligence Uses Metadata to Map Adversary Networks. (2013, 8 July). *Defense news*. http://www.defensenews.com/article/20130708/C4ISR02/307010020. Accessed October 20, 2013.

Miller, G., Brennan Speech Is First Obama Acknowledgement of the Use of Armed Drones. (2012a, 30 April). *The Washington Post*. http://articles.washingtonpost.com/2012-04-30/world/35452340_1_drone-strikes-drone-program-brennan-speech. Accessed October 20, 2013.

Miller, G., Plan for Hunting Terrorists Signals US Intends to Keep Adding Names to Kill Lists. (2012b, 23 October). *The Washington Post*. Accessed October 20, 2013.

Murdock, D. G., Tomes, R. R., & Tucker, C. K. (2014). *Human geography. Socio-cultural dynamics and challenges to global security*. Herdon, VA: United States Geospatial Intelligence Foundation.

Nikiforakis, N., Kapravelos, A., Joosen, W., Kruegel, C., Piessens, F., & Vigna, G. (2013). Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In *Security and privacy (SP), 2013 IEEE symposium on, 19–22 May 2013* (pp. 541–555). doi:10.1109/SP.2013.43.

Quinn, K. (2012). A better toolbox. *Trajectory Magazine,* Winter. http://trajectorymagazine.com/defense-inteligence/item/1349-a-better-toolbox.html. Accessed October 20, 2013.

Richards, N. M., & King, J. H. (2013). Three paradoxes of Big Data. *Stanford Law Review Online, 41*(September 3), 41–46.

Richelson, J. T. (1995). *A century of spies. Intelligence in the twentieth century*. New York: Oxford University Press.

Richelson, J. T. (2012). *The US intelligence community* (6th ed.). Boulder, CO: Westview Press.

Risen, J., & Poitras, L., NSA Gathers Data on Social Connections of US Citizens. (2013, September 28). *The New York Times*. http://nyti.ms/1fxW2c6. Accessed October 17.

Roy, N., Wang, H., & Choudhury, R. R. (2014). I am a smartphone and i can tell my user's walking direction. In *Proceedings of the 12th international conference on Mobile systems, applications, and services*, *MobiSys 14*. (pp. 329–342). ACM.

Schwartz, R., & Halegoua, G. R. (2014). The spatial self: Location-based identity performance on social media. *New Media & Society,*. doi:10.1177/1461444814531364.

Singer, P. W. (2009). *Wired for war. The robotics revolution and conflict on the 21st century*. New York: Penguin Books.

Soltani, A., & Gellman, B., New Documents Show How the NSA Infers Relationships Based on Mobile Location Data. (2013, December 10). *The Washington Post*. http://wapo.st/1hrSi9F.

Soltani, A., Peterson, A., & Gellman, B., NSA Uses Google Cookies to Pinpoint Targets for Hacking. (2013, December 10). *The Washington Post*. http://wapo.st/1d7oCvx.

Sorenson, J., Big Data: How to Fulfill the Promise of Limitless Intelligence. (2013, 19 September). *C4ISR&Networks*. http://www.c4isrnet.com/article/20130919/C4ISRNET18/309190007. Accessed October 20, 2013.

Surden, H. (2007). Structural rights in privacy. *Southern Methodist University Law Review, 60*, 1605–1629.

U.S. Government. (2013). *US policy standards and procedures for the use of force in counterterrorism operations outside the United States and areas of active hostilities.* Washington DC: Office of the President.

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review, IV*(5), 193–220.

Wilson, M. W. (Forthcoming). New Lines? Enacting a social history of GIS. *The Canadian Geographer/Le Géographe canadien*.