THE DAWN OF SOCIAL INTELLIGENCE (SOCINT)

*Laura K. Donohue**

ABSTRACT

More information about citizens' lives is recorded than ever before. Because the data is digitized, it can be accessed, analyzed, shared, and combined with other information to generate new knowledge. In a post-9/11 environment, the legal standards impeding access to such data have fallen. Simultaneously, the advent of global communications and cloud computing, along with network convergence, have expanded the scope of information available. The U.S. government has begun to collect and to analyze the associated data.

The result is the emergence of what can be termed "social intelligence" (SOCINT), which this Article defines as the collection of digital data about social relationships. What distinguishes this type of information from more traditional forms of intelligence is that it draws from novel, digitized sources, such as metadata, social media, and geolocational information, to construct a detailed picture of networks—which themselves then serve as starting points for further analysis. The telephony metadata program initiated under Section 215 of the USA PATRIOT Act provides one prominent example. Numerous other initiatives are underway. These collection programs carry significant risks. The construction of ZunZuneo demonstrates how SOCINT can be used not just to understand social dynamics, but to drive political, economic, or social change. As a constitutional matter, the broad collection of social data is at cross-purposes with the Fourth Amendment, with sobering consequences for individual rights. SOCINT thus ought to be treated as a form of collection in its own right, subject to unique restrictions, and not as a concomitant of other collection techniques.

TABLE OF CONTENTS

* Professor of Law, Georgetown Law; Director, Georgetown Law Center on National Security and the Law; Director, Georgetown Law Center on Privacy and Technology. Special thanks to the editors of the Drake Law Review for their assistance.

I. INTRODUCTION

Technology is altering the amount and type of information that can be known about citizens, with profound implications for privacy. A vast quantity of personal data is now digitized. Peoples' lives are recorded by businesses; employers; local, state, and federal agencies; friends and family; and themselves. Cameras owned by private and public entities capture their movement in public space. Where they go, what they buy, what they read, with whom they interact, and the nature of their relationships with others are reflected in the digital sphere.

The recording of this information means three things. First, it can be accessed. This is not a trivial consideration. Information that was not available now is, and it exists in quantities that dwarf what previously could have been known.[1] Second, it can be analyzed at a level never before conceived.[2] Advances in mathematics and network design mean that sophisticated algorithms can be applied to the information to generate new knowledge. In the process, those with access to the data can learn things that people do not even know about themselves. Third, and relatedly, because

1. *See, e.g.*, *Data, Data Everywhere*, THE ECONOMIST (Feb. 25, 2010) http://www.economist.com/node/15557443 ("Wal-Mart, a retail giant, handles more than 1 million customer transactions every hour, feeding databases estimated at more than 2.5 petabytes—the equivalent of 167 times the books in America's Library of Congress . . . ."); *The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things: Executive Summary*, IDC (Apr. 2014), http://www.emc.com/leadership/digital-universe/2014iview/executive-summary.htm (stating the staggering amount of digital data has reached new thresholds and noting the amount of data is doubling in size every two years).

2. *See, e.g.*, Luca Cagliero & Alessandro Fiori, *Knowledge Discovery from Online Communities*, *in* SOCIAL NETWORKING AND COMMUNITY BEHAVIOR MODELING: QUALITATIVE AND QUANTITATIVE MEASURES 123, 124 (Maytham Safar & Khaled A. Mahdi eds., 2012).

private information exists in a digital sphere, other information can be combined to deepen the understanding of the recorded data. Paralleling these changes, resource limitations that silently played a restraining role are just as quietly slipping away.

One of the most profound types of insight that can be generated from the digital world relates to social networks: connections between individuals and organizations that shed light on the social fabric, creating an object that can be observed, analyzed, and potentially, manipulated.[3] The structure can be gleaned from electronic communications that range from telephones to computer-based interactions, such as Voice over Internet Protocol (VoIP), email, chat rooms, and gaming networks.[4] Social media sites such as Twitter, Snapchat, and Instagram, provide insight into connectedness between individuals, adding content that reveals beliefs, interests, and predilections—as well as what individuals have done and would like to do.[5] Even traditional modes of communications, such as letters sent through the ordinary post, are not immune—the government records and digitizes envelope information.[6] Employment data, housing information, political contributions, religious observance, and participation in organizations that maintain a web presence offer further ways to document the extent and qualities of social, political, and economic communities.[7]

The most salient question in analyzing social network data is not what can be studied, but where to draw the line.[8] So much information is now available that one can construct a model of relationships within any conceivable community, filling out the picture with the nature of the

3. *See id.*

4. *See, e.g.*, Joe Pappalardo, *NSA Data Mining: How It Works*, POPULAR MECHANICS (Sept. 11, 2013), http://www.popularmechanics.com/military/a9465/nsa-data-mining-how-it-works-15910146/ (noting the NSA PRISM program collects information from "digital photos, stored data, file transfers, emails, chats, videos, and video conferencing").

5. *See* Cagliero & Fiori, *supra* note 2, at 124–25.

6. *See* Ron Nixon, *U.S. Postal Service Logging All Mail for Law Enforcement*, N.Y. TIMES (July 3, 2013), http://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html?_r=o.

7. *See* Mary Edwards, *Community Guide to Development Impact Analysis*, WISC.EDU, http://www.lic.wisc.edu/shapingdane/facilitation/all_resources/impacts/analysis_socio.htm (last visited Oct. 1, 2015).

8. *See, e.g.*, Jenna Wortham, *When the Web's Chaos Takes an Ugly Turn*, N.Y. TIMES (Oct. 20, 2012), http://www.nytimes.com/2012/10/21/technology/a-reddit-forum-prompts-questions-of-where-to-draw-a-line.html.

interests that tie individuals together. Even relationships between regions or countries can be explored, in the process providing details on the nature and quality of the connections. The promise of "Big Data," as it has come to be called, offers insight into the broadest, and the most minute, aspects of the social order.[9]

Numerous sectors are keen to take advantage of the opportunities offered by these new technologies.[10] Industry is capitalizing on it, using the information generated to sell products and services that customers did not even realize they wanted. So when Amazon.com suggests, "other books you might like," it turns out, you do.[11]

Individuals are using it to connect to friends, and friends of friends, finding others with similar interests and creating worldwide communities. The social aspect of such networks offers connectedness. It offers opportunities to learn. It provides individuals with the chance to explore worlds that previously would not be accessible.

The government, in turn, sees in Big Data opportunity for the more effective provision of services.[12] It looks to it as a way to conduct better investigations for law enforcement purposes.[13] And it seeks to realize the potential of not just detecting, but *preventing* future threats to national security.

The foreign intelligence realm, in particular, has begun to shift its emphasis to Big Data as a way to identify and to respond to threats to national security. What is being created is a form of "social intelligence," or SOCINT, which is broadly defined here as the collection of digital data

9. Jonathan Shaw, *Why "Big Data" Is a Big Deal*, HARV. MAG. (Apr. 2014), http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal.

10. Boris Dzhingarov, *Social Media: How Major Industries Take Advantage of the Emerging Content Platform*, SOCIALNOMICS (June 24, 2015), http://www.socialnomics.net/2015/06/24/social-media-how-major-industries-take-advantage-of-the-emerging-content-platform/.

11. *See* Thomas H. Davenport, Leandro Dalle Mule & John Lucker, *Know What Your Customers Want Before They Do*, HARV. BUS. REV. (Dec. 2011), http://hbr.org/2011/12/know-what-your-customers-want-before-they-do; Stephen Goldsmith, *Big Data, Analytics and a New Era of Efficiency in Government*, GOVERNING (May 22, 2013), http://www.governing.com/blogs/bfc/col-big-data-analytics-government-efficiency.html.

12. *See, e.g.*, Goldsmith, *supra* note 11.

13. *See, e.g.*, Bryce Clayton Newell, *Local Law Enforcement Jumps on the Big Data Bandwagon: Automated License Plate Recognition Systems, Information Privacy, and Access to Government Information*, 66 ME. L. REV. 397, 398 (2014).

about social relationships.[14] Notably, the U.S. intelligence community does not appear to separate digital social intelligence from other forms of information.[15] Nor has Congress sought specifically to legislate in this area. To the contrary, the government has gone through legal gymnastics to read the authority to collect certain forms of SOCINT in a manner compatible with the 1978 Foreign Intelligence Surveillance Act.[16] To the extent that SOCINT is not addressable through the current statutory regime, Executive Order 12333 and the associated directives remain the framing.[17]

Changes in foreign intelligence collection, as well as global communications structures, have facilitated the extension of intelligence gathering to SOCINT. In the former area, since October 2001, there has been a weakening of the legal standards limiting access to citizens' data.[18] In

14. SOCINT is used here as a potential intelligence moniker akin to HUMINT (human intelligence), SIGINT (signals intelligence), or OSINT (open source intelligence). For a list of the various sources of intelligence collection, see *Intelligence Collection Disciplines*, FBI, https://www.fbi.gov/about-us/intelligence/disciplines (last visited Oct. 1, 2015).

15. Instead, information that reveals social relationships is gleaned from other types of intelligence gathering, such as OSINT (open source intelligence), and SIGINT, which includes both COMINT (communications intelligence, i.e., information gleaned from conversations between individuals), and ELINT (electronic intelligence, i.e., data obtained from electronic signals that are not themselves a direct part of communications). *See* Headquarters, Dep't of US Army, *Open Source Intelligence*, Army Techniques Publication No. 2-22.9 (July 10, 2012), *available at* https://fas.org/irp/doddir/army/atp2-22-9.pdf; *Intelligence Collection Disciplines*, *supra* note 14 (defining SIGINT); RICHARD L. BERNARD, NSA, ELECTRONIC INTELLIGENCE (ELINT) AT NSA 1 (2009), https://www.nsa.gov/about/_files/cryptologic_heritage/publications/misc/elint.pdf (defining ELINT); *see also* KERRY PATTON, SOCIOCULTURAL INTELLIGENCE: A NEW DISCIPLINE IN INTELLIGENCE STUDIES 11–12 (2010). *But see* David Omand, *Understanding Digital Intelligence: A British View*, *in* NATIONAL SECURITY AND COUNTERINTELLIGENCE IN THE ERA OF CYBER ESPIONAGE (Eugenie de Silva, ed., forthcoming January 2016) (distinguishing digital intelligence); David Omand, Jamie Bartlett, & Carl Miller, *Introducing Social Media Intelligence*, 27 INTELLIGENCE & NAT'L SECURITY 801, 803–23 (2012) (distinguishing social media intelligence).

16. *See* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 836–38 (2014) [hereinafter Donohue, *Metadata Collection*] (discussing redefinition of "relevant" to allow for the bulk collection of telephony metadata under FISA's business records provision); *see also* CHARLIE SAVAGE, POWER WARS: INSIDE OBAMA'S POST-9/11 PRESIDENCY 197, 201–201, 205–206 (2015) (discussing redefinition of "relevant," "facility," and "target" to allow for the broad collection of social data under separate sections of FISA).

17. *See* Exec. Order No. 12,333, 3 C.F.R. § 1981 (Dec. 4, 1981).

18. *See* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-

the latter area, network convergence and the structure of global communications have further eroded barriers to collection. It used to be that foreign countries communicated with their agents over specialized network.[19] Human intelligence reports, military dispatches, diplomatic instructions, and signals data were relayed through individualized routes.[20] To intercept information, agents had to find a way to break into these systems.

Foreign countries' communications, however, are no longer restricted to separate networks.[21] Instead, the same systems used daily by ordinary citizens carry foreign intelligence traffic.[22] Simultaneously, the threat posed by non-state actors has increased.[23] To locate and monitor these threats, the government has increasingly focused on systems carrying citizens' private communications.[24] Another aspect of network convergence expands the privacy interests implicated: it is not just one kind of communication carried via the Internet, but telephone, video, signals, and data all travel over its paths.[25] As the so-called "Internet of Things" takes hold, the privacy interests will only deepen.[26]

458, § 6001(a), 118 Stat. 3638, 3742 (codified as amended at 50 U.S.C. § 1801 (2012)); Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 206, 115 Stat. 272, 282 (codified as amended at 50 U.S.C. § 1805(c)(2)(B) (2012)); EDWARD C. LIU, CONG. RESEARCH SERV., R40138, AMENDMENTS TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA) EXTENDED UNTIL JUNE 1, 2015, at 1–2 (2011), *available at* https://www.fas.org/sgp/crs/intel/R40138.pdf; *see also generally* LAURA K. DONOHUE, THE COST OF COUNTERTERRORISM: POWER, POLITICS, AND LIBERTY (2008); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015) [hereinafter Donohue*, International Content*]; Donohue, *Metadata Collection*, *supra* note 16.

19. *See, e.g.*, *The Evolution of the U.S. Intelligence Community—An Historical Overview*, FAS (Feb. 23, 1996), http://fas.org/irp/offdocs/int022.html (detailing a brief history of the development of the United States intelligence community and surveillance of foreign communications).

20. *See id.*

21. *See* RICHARD A. CLARKE, ET. AL, THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD xi–xii (2014).

22. *See id.*

23. *See id.* at 27–30.

24. *See id.* at xii.

25. *See* Mark Elmore, *Comment, Big Brother Where Art Thou, Electronic Surveillance and the Internet: Carving Away the Fourth Amendment Privacy Protections*, 32 TEX. TECH L. REV. 1053, 1054-56 (2001).

26. *See* Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward*

The structure of global communications themselves has also changed. Traditionally, domestic communications were provided with a higher level of protection than those carried internationally.[27] But new technologies have broken down the distinction, with the result that a significant amount of domestic communications traverse U.S. borders, at which point they become subject to collection.[28] In the face of cloud computing, even static data, such as photographs, papers, and financial records, may be held on servers overseas.[29]

In brief, an increasing amount of information about individuals' lives is digitized. It can be accessed, analyzed, and combined with other data to generate insight into society.[30] Simultaneously, changes in the foreign intelligence collection and global communications structures mean that the government now has broad access to this information.[31]

This Article argues that the collection of digital social data, which can be combined with other information and queried to produce knowledge, and which is vulnerable to manipulation, represents a new form of intelligence. In the post-9/11 world, the growth of SOCINT carries significant risks and has catapulted the country along a dangerous path. In taking this direction, the government is undermining bedrock principles on which the United States was founded.

The Article begins by distinguishing SOCINT from other forms of intelligence gathering by positing three core characteristics: (a) the collection of non-traditional forms of digital data with deep implications for citizens' privacy, (b) the function of SOCINT as a starting point for analysis of the social order, and (c) the potential use of the data to neutralize actors or to effect large-scale social, political, and economic change.[32]

Managing Discrimination, Privacy, Security, and Consent, 93 TEX. L. REV. 85, 132 (2014).

27. *See* Donohue, *Metadata Collection*, *supra* note 16, at 766–67.

28. *See id.*

29. *See* Axel Amback & Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad*, 21 MICH. TELECOMM. & TECH. L. REV. 317, 321 (2015).

30. Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet*,' THE GUARDIAN (July 31, 2013) [hereinafter Greenwald, *XKeyscore*], http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data/print.

31. *See id.*

32. *See infra* Part II.

The Article next recognizes the absence of a sufficient statutory framing for the collection of this type of data, providing an example of how one recent program, the collection of telephony metadata under Section 215 of the USA PATRIOT Act, violated the Foreign Intelligence Surveillance Act (FISA).[33] It then details some of the social intelligence programs currently being conducted under Section 702 of the FISA Amendments Act, as well as Executive Order 12333, highlighting in the process the depth of the privacy interests involved.[34]

The Article then turns to the dangers of SOCINT.[35] The nonstatic nature of social networks and their vulnerability to manipulation increase the risks of allowing broad access to social network data.[36] With little regard for political boundaries, instantaneous communication, and the potential leverage of massive human resources, social networks can be used to affect political, social, and economic change. The United States Agency for International Development's (USAID) effort to launch ZunZuneo in Cuba provides an example of how the U.S. government has tried to construct and use social networks for political aims.[37]

From this, the Article highlights the constitutional concerns evinced in the course of social intelligence collection, noting that the purpose of the Fourth Amendment was to eliminate general warrants.[38] These instruments were used to collect information prior to any evidence of wrongdoing, with the attendant danger that the information—particularly information about relationships—could then be used to head off opposition.[39] The case of Paul Revere provides a powerful example of the strength of SOCINT and its potentially profound impact.[40] The underlying rights questions also matter. The collection of social data may impact qualities otherwise protected by liberal democratic states, such as the importance of solitude and self-determination, the need to allow for democratic deliberation, and the attendant rights of freedom of speech and freedom of association.[41]

33. *See infra* Part III.
34. *See id.*
35. *See infra* Part IV.
36. *See id.*
37. *See id.*
38. *See infra* Part V.
39. *See id.*
40. *See id.*
41. *See id.*

The Article concludes by recognizing that whatever one may think about SOCINT, the fact that it is such a powerful tool—and one replete with underlying constitutional risks—means, at a minimum, that it deserves direct analysis and attention and not to be treated as a concomitant of other forms of intelligence gathering.[42] What is needed is a stronger statutory framing, removing SOCINT from the sole domain of Executive Order 12333, or as an ancillary to FISA §702.

II. DEFINING SOCIAL INTELLIGENCE

Social intelligence (SOCINT), the collection of digital data about social relationships, differs from other forms of intelligence gathering in three critical ways.

First, SOCINT relies on non-traditional, digitized data, which includes social media, communications metadata, and geolocational information. The first category further subdivides into at least three areas: social sites, collaborative platforms, and interest-group formation.

Social media sites like Facebook, LinkedIn, Instagram, and Snapchat, as well as dating sites like Match.com, eHarmony, and Lovestruck, are designed *to create connections* between people.[43] These sites are a product of the digital revolution, and they have attracted an enormous amount of attention. Match.com started in 1995.[44] By 2004, it had registered more than 42 million users.[45] It now has approximately 24 million users at any one time.[46] It is only one of myriad dating sites. According to the company, some

42. *See infra* Part VI.

43. *See Social Media*, MERRIAM-WESBSTER DICTIONARY, http://www.merriam-webster.com/dictionary/social%20media (last visited Nov. 1, 2015) (defining social media as "forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)).

44. *See About Match.com*, MATCH.COM, http://www.match.com/help/aboutus.aspx?lid=4 (last visited Oct. 31, 2015).

45. *It's a Record Breaker; Guinness Says Match.com Leads the World in Online Dating*, SOURCEWIRE NEWS DISTRIBUTION (Nov. 22, 2004), http://www.sourcewire.com/news/20013/it-s-a-record-breaker-guinness-says-match-com-leads-the#.Vi99yMuqdfQ.

46. *Online Dating Statistics*, STATISTIC BRAIN RESEARCH INSTITUTE (Sept. 18, 2015), http://www.statisticbrain.com/online-dating-statistics/ (compiling statistics regarding online or Internet dating from Reuters, Herald News, PC World, and the Washington Post).

forty million Americans regularly use online dating services.[47] In January 2004, Facebook did not even exist.[48] It formally became Facebook.com in August 2005.[49] Just one decade later, on August 27, 2015, *one billion* users signed onto the site.[50] According to founder and CEO Mark Zuckerberg, Facebook maintains 1.5 billion monthly users.[51]

Social media reaches beyond sites designed to create networks to include collaborative platforms—i.e., websites and apps that enable people to create and to share content.[52] Sites that may not appear on their face as serving in a social network capacity may act similarly to bring people together. Google+, for instance, tries to enable "real-life sharing" via the Internet.[53] It has 11 million followers.[54] Wikipedia, a free encyclopedia derived solely through collaborative editing, brings together communities of interest around the topics listed, with thousands of edits entered hourly.[55]

Social media also includes sites dedicated to the formation of interest groups. Initially, many of these simply provided users with access to products or services, such as music, photos, news stories, or games. But some have now evolved to build networks through common interests. Spotify users, for instance, can now share playlists.[56] At Shutterfly, groups can be formed,

47. Meredith Broussard, *Dating Stats You Should Know*, MATCH.COM (Oct. 27, 2015), http://www.match.com/magazine/article/4671/; *see also Online Dating Statistics*, *supra* note 46.

48. *See* Sarah Phillips, *A Brief History of Facebook*, THE GUARDIAN (July 25, 2007), http://www.theguardian.com/technology/2007/jul/25/media.newmedia.

49. *Id.*

50. Julia Greenberg, *1 Billion People Used Facebook on Monday*, WIRED (Aug. 27, 2015), http://www.wired.com/2015/08/1-billion-people-used-facebook-monday/.

51. *Id.*

52. *See Social Media*, *supra* note 43 (defining social media as "forms of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos)).

53. *Google+ Features*, GOOGLE, http://www.google.com/intl/en/+/learnmore/circles/ (last visited Oct. 31, 2015).

54. *Google+*, GOOGLE, https://plus.google.com/+googleplus/about (last visited Nov. 1, 2015).

55. *Wikipedia: Introduction*, WIKIPEDIA, https://en.wikipedia.org/wiki/Wikipedia:Introduction (last visited Nov. 1, 2015).

56. *See About Us*, SPOTIFY, https://www.spotify.com/us/about-us/contact/ (last visited Oct. 31, 2015); *How Do I Share Music With My Friends?*, SPOTIFY, https://support.spotify.com/us/learn-more/guides/#!/article/sharing-music (last visited Oct. 31, 2015).

giving the members access to the same images and announcements,[57] while at Reddit, individuals can subscribe to subreddits to follow and to help drive the top stories.[58] Even gaming communities can now come together while in the game itself, communicating with players half a world away. Thus, Overwolf features "a wide variety of epic apps, made by gamers," to import social media. [59] The company promotes a JavaScript based software development kit (SDK) called KAIGOS (Kick Ass In Game Operating System), to encourage gamers to develop yet more apps for in-game social networking.[60]

What is notable about social media sites is that they take private relationships and put them online. Beyond this, they create new relationships, which become digitally imprinted on the electronic sphere. So entire communities that never before existed have now come into being. And because they are digitized, they are accessible.

Social media is not the only non-traditional form of data that contributes to SOCINT. It also may derive from communications metadata—that is, patterns in relationships that can be generated by paying attention to what individuals do in the course of their daily lives. Revealing whom one happens to call has not traditionally been regarded as particularly intimate data.[61] But as the telephone has become more central to our lives, and the volume of calls between individuals has exponentially increased, more and more information can be gleaned from the length and frequency of contact, as well as patterns in calls.[62] Private details about individuals' lives, and the broader networks within which they operate, can be uncovered by looking at other forms of communications metadata as well, such as email,

57. *See Share Sites*, SHUTTERFLY, https://www.shutterfly.com/sites/create/welcome.sfly?fid=7e3ac6c333a10e40 (last visited Oct. 31, 2015).

58. *See* Jacob O'Gara, *Reddit 101: A Beginner's Guide to the Front Page of the Internet*, DIGITAL TRENDS (Dec. 20, 2013), http://www.digitaltrends.com/social-media/reddit-101/.

59. *About Overwolf*, OVERWOLF, http://www.overwolf.com/about-overwolf/ (last visited Oct. 31, 2015).

60. *Id.*

61. *See* Donohue, *Metadata Collection*, *supra* note 16, at 863–65 (discussing *Smith v. Maryland* where the Supreme Court found an individual does not have a reasonable expectation of privacy in the numbers dialed from one's telephone).

62. Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, WEB POLICY (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

text messaging, Skype, instant chats, and Internet browsing.[63]

Another new source of social information centers on geolocational data, which can be gleaned from a variety of sources, such as radio-frequency identification (RFID) chips, global positioning systems, trunk identifier information, license plate readers, or CCTV paired with biometric identification systems.[64] This type of information can reveal not just where an individual goes, and when they go there, but who they are with when they do so.[65] These novel forms of data can be used to map social relationships.

Second, SOCINT differs from traditional forms of intelligence in that it can serve as a starting point for socio-cultural knowledge generation.[66] Owing to its volume, the sophistication of the algorithms that can be run on data, the types of information with which it can be combined (because it is both ordered and digitized), and the type of knowledge that can be generated, SOCINT goes well beyond what would have been digestible in a world of human intelligence (HUMINT) or even signal intelligence (SIGINT). Insights about which even the objects of the analysis may have little or no knowledge can be gleaned. In contrast, in traditional SIGINT, the parties to the communication are aware of what has been said.[67] But those who form the nodes in SOCINT may be utterly ignorant of what can be gleaned from their behavior, as well as their relationship to other individuals and organizations in the network.

The third distinguishing factor of SOCINT is that the data itself can be used to effect widespread political, economic, or social change.[68] This is primarily done through using the data collected to identify critical nodes in the networks, which can then be neutralized, pressured, or otherwise

63. *See* Steven J. Vaughan-Nichols, *Big Data, Metadata, and Traffic Analysis: What the NSA is Really Doing*, ITWORLD (July 26, 2013), http://www.itworld.com/article/2829511/big-data/big-data—metadata—and-traffic-analysis—what-the-nsa-is-really-doing.html.

64. *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 420–37 (2012).

65. *See id.*

66. *See* PATTON, *supra* note 15, at xiii; *see also* LEEELLEN FRIEDLAND, GARY W. SHAEFF & JESSICA GLICKEN TURNLEY, SOCIO-CULTURAL PERSPECTIVES: A NEW INTELLIGENCE PARADIGM, REPORT ON THE CONFERENCE AT THE MITRE CORPORATION MCLEAN, VIRGINIA, SEPTEMBER 12, 2006 (June 2007), *available at* http://www.mitre.org/sites/default/files/pdf/07_1220.pdf.

67. *See supra* note 15 and accompanying text.

68. *See* discussion *infra* Part IV.

persuaded to act in ways that use or fundamentally change the surrounding social network. It can do this because of the nature of digital networks. Social media provides a rich and diverse source of information that can be disseminated quickly, with little regard for geopolitical boundaries. Communication among participants can happen almost instantaneously, outside traditional regulatory regimes. And it can involve large numbers of people, which means that significant human resources can be mobilized.

Because of these unique characteristics (the collection of novel forms of digital data with deep privacy implications, the use of SOCINT as a starting point for knowledge production, and the potential use of social intelligence to neutralize opposition or to effect political, economic, or social change), the power encapsulated in SOCINT goes well beyond the collection of other forms of intelligence. It constitutes a new type of knowledge.

The collection of this data has massive implications. The power of social networks is gradually becoming apparent.[69] One need look no further than the 2001 convergence of protestors in Manilla, which prompted the Philippine Congress to change its course and to impeach Philippine President Joseph Estrada.[70] In Spain, demonstrations generated by text messaging resulted in the departure of Spanish Prime Minister José María Aznar.[71] The overthrow of the autocratic governments in Tunisia and Egypt in early 2011, known broadly as the "Arab Spring," similarly relied on social networks for their execution.[72] The risk is that individuals who can map and control such networks can accomplish massive changes in political, economic, and social structures.

III. ABSENCE OF SUFFICIENT STATUTORY FRAMING

The framing for U.S. foreign intelligence collection falls into two broad (and at times overlapping) categories: the 1978 Foreign Intelligence Surveillance Act (as amended), [73] and Executive Order 12333, first

69. *See* Clay Shirky, *The Political Power of Social Media: Technology, the Public Sphere, and Political Change*, FOREIGN AFF. (Jan./Feb. 2011), https://www.foreignaffairs.com/articles/2010-12-20/political-power-social-media.

70. *Id.*

71. *Id.*

72. *See generally* PHILIP N. HOWARD ET AL., OPENING CLOSED REGIMES: WHAT WAS THE ROLE OF SOCIAL MEDIA DURING THE ARAB SPRING? (2011), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2595096.

73. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783

introduced by President Reagan in 1981.[74] The former initially addressed only electronic communications.[75] Congress later expanded the statute to cover physical searches,[76] the use of pen register and trap and trace devices,[77] and the acquisition of business records.[78] Post-9/11, the business records provision was altered to allow the government to obtain tangible goods.[79] Together, these authorities are referred to as "Traditional FISA."

In 2008, the Administration convinced Congress that alterations to FISA were required to take account of the global nature of communications.[80] The problem, the government argued, was that communications previously considered international, and thus not subject to FISA, might pass through the United States, thus forcing the intelligence community to go to the Foreign Intelligence Surveillance Court for intercept permission. Accordingly, the government altered the statute to construct what is referred to as "Modern FISA," which gives the government greater leeway when the target of the intercept is believed to be a non-U.S. person based outside the United States.[81]

(codified as amended at 50 U.S.C. §§ 1801–1885c (2012)).

74. Exec. Order No. 12,333, 3 C.F.R. § 1981 (Dec. 4, 1981).

75. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 102, 92 Stat. 1783, 1786–88.

76. Intelligence Authorization Act for Fiscal Year 1995, Pub L. No. 103-359, § 807, 108 Stat. 3423, 3443–53 (1994) (codified at 50 U.S.C. §§ 1821–1829) (physical searches).

77. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404–10 (1998) (codified at 50 U.S.C. §§ 1841–1846) (pen register and trap and trace devices).

78. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2410–12 (1998) (codified at 50 U.S.C. §§ 1861–1863) (business records). Various other amendments have been made. The USA PATRIOT Act, for instance, Section 207 changed the duration of certain FISA authorization orders; Section 208 increased the number of FISC judges to 11; Section 214 amended FISA pen register and trap and trace provisions; Section 218 changed the purpose of electronic & physical searches; and Section 504 authorized coordination between intelligence and law enforcement. ITRPA subsequently added a "lone wolf" provision via § 6001. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742 (codified at 50 U.S.C. § 1801(b)(1) (2012)).

79. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861 (2012)) (tangible goods).

80. *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

81. *See id.*

FISA does not directly address the collection of social intelligence.[82] Instead, efforts have been made to shoehorn communications metadata collection into the business records, as well as pen register and trap and trace provisions, of Traditional FISA.[83] Such efforts proved ill founded. At the same time, the intelligence community has created collection programs under Modern FISA that include significant amounts of information about U.S. citizens' social networks.[84]

Outside of the FISA regime, Executive Order 12333, and its associated directives, provide the framing for surveillance programs that are heavily dependent on digitized social data.[85] The order, however, lacks sufficient particularity for handling the unique challenges of this type of information.

A. *Telephony Metadata Collection Under Section 215*

In June 2013, the *Guardian* published a copy of an order issued by the Foreign Intelligence Surveillance Court[86] requiring Verizon to turn over "an electronic copy of the following tangible things: all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." [87] The order heralded the intelligence community's entry into social intelligence collection in all but name. To find the authority to collect telephony metadata, the government interpreted the law in a manner that stretches credulity.

When the order first reached the public domain, there was some confusion over its legal justification. [88] Traditionally, the intelligence

82. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1885c (2012)).

83. *See* discussion *infra* Part III(A)–(B).

84. *See id.*

85. Exec. Order No. 12,333, 3 C.F.R. § 1981 (Dec. 4, 1981).

86. *Verizon Forced to Hand over Telephone Data—Full Court Ruling*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

87. *In re* Application of F.B.I. for an Order Requiring the Production of Tangible Things From Verizon Bus. Network Servs., Inc., No. 13-80, at 2 (FISA Ct. 2013) [hereinafter In re *Application of F.B.I*], *available at* http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

88. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

community had to demonstrate that the person about whom it was obtaining information was a foreign power or an agent of a foreign power before collection could commence.[89]

What the Verizon order suggested was that collection did not have to be particularized.[90] Intelligence agencies were collecting massive amounts of data to *look* for potential threats to the United States.[91] The order, moreover, explicitly included telephone calls "wholly within the United States, including local telephone calls."[92] Although previously a higher level of protection had been extended to the collection of domestic content,[93] under the terms of the order, no such distinguishing factor appeared to be applied in this case.[94]

One clue to the order's presumed legal nexus appeared in the phrase "tangible things."[95] The term hearkens back to a clause added to the 1978 Foreign Intelligence Surveillance Act (FISA) in the aftermath of 9/11.[96] But before the iconic USA PATRIOT Act weakened the constraints on the intelligence community, this section of FISA was known as the business records provision, introduced in response to an earlier terrorist attack.[97]

In 1995, a right-wing extremist, Timothy McVeigh, placed a Ryder rental truck packed with a fertilizer bomb outside the Murrah Federal Building in Oklahoma City.[98] The explosion left 168 people dead and

89. *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1885c (2012)).

90. *See* In Re *Application of F.B.I.*, *supra* note 87.

91. *See Based on What We Know, Is the NSA Verizon Request Legal?*, NPR.ORG (June 15, 2013), http://www.npr.org/sections/thetwo-way/2013/06/15/191619038/based-on-what-we-know-is-the-nsa-verizon-request-legal.

92. *See* In Re *Application of F.B.I.*, *supra* note 87.

93. Donohue, *Metadata Collection*, *supra* note 16, at 806.

94. *See id.* at 803–04.

95. *See* In Re *Application of F.B.I.*, *supra* note 87.

96. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861 (2012)).

97. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2411–12 (codified as amended at 50 U.S.C. §§ 1861–1863 (2012)).

98. Douglas O. Linder, The Oklahoma City Bombing & the Trial of Timothy McVeigh (UMKC School of Law, Faculty Project 2006), http://law2.umkc.edu/faculty/projects/ftrials/mcveigh/mcveighaccount.html.

hundreds more injured.[99] During the investigation, prosecutors were not clear on whether they had the authority to obtain McVeigh's business records related to the truck rental, a storage unit that he maintained in Kansas, and his locker in Arizona.[100] Although the attack was domestic, Congress altered FISA to authorize the production of certain types of business records related to individuals suspected of being foreign powers or agents of a foreign power.[101]

Under the statute, applications for a court order had to "specify that . . . the records concerned [were] sought for an investigation [to gather foreign intelligence information or an investigation concerning international terrorism]; and there [were] specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[102] To limit the reach of orders, any records sought had to be for "an investigation to gather foreign intelligence information or an investigation concerning international terrorism."[103] The application established the potential involvement of the target in illegal activities.[104] Congress required intelligence agencies to follow the same steps as those taken with regard to electronic surveillance—submitting an application to FISC to obtain an order, which then compels the company to hand over the records.[105]

The statute limited the types of businesses on which the court could serve orders to include only common carriers, public accommodation

99. *Id.*

100. *See* Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1329 (2004) (noting that in 1998 FISA was extended to include the kind of business records relevant to the Oklahoma City bombing investigation).

101. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2411–12 (codified as amended at 50 U.S.C. § 1862 (2012)).

102. *Id.* at § 602, 112 Stat. at 2411.

103. *Id.*

104. *Id.* As with the other provisions of traditional FISA, Congress assigned the terms "foreign power," "agent of a foreign power," "foreign intelligence information," and "international terrorism" the same meanings as employed in relation to electronic surveillance. *Compare* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, §101(a)–(c), (e), 92 Stat. 1783, 1783–84 (codified as amended at 50 U.S.C. 1801 (2012)), *with* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2411 (codified as amended at 50 U.S.C. § 1861 (2012)).

105. *Compare* Pub. L. No. 95-511, §102, 92 Stat. 1783, 1786–88, *with* Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2411–12.

facilities, storage facilities, and vehicle rental facilities.[106] Even so, the number of entities implicated was considerable. Common carriers includes any individual or company that transports people or things on regular routes, at set rates.[107] It covers buses, taxis, commercial airplanes, passenger trains, cruise ships, railroads, and trucking companies.[108] According to the DOJ, "places of public accommodation," in turn, include more than 5 million establishments in the United States, "such as restaurants, hotels, theaters, convention centers, retail stores, shopping centers, dry cleaners, laundromats, pharmacies, doctors' offices, hospitals, museums, libraries, parks, zoos, amusement parks, private schools, day care centers, health spas, and bowling alleys."[109] With regard to storage facilities, by 2015, there were more than 48,500 units, constituting the fastest growing segment of the commercial real estate industry over the past four decades.[110] Finally, as of 2014, car rental companies were in more than 21,000 locations, offering consumers access to more than 2 million cars.[111] These companies reach into Americans' daily lives, offering insight into matters ranging from medical issues and intimate relationships to financial conditions and travels.

Despite claiming the necessity of the business records provision, the executive branch made little use of it, filing an application with FISC only once between 1998 and 2001.[112]

Section 215 of the USA PATRIOT Act expanded what types of information could be obtained under the business records provision.[113] The

106. *See* Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2411–12.

107. *Id.* at § 602, 112 Stat. at 2411.

108. *See What is a Common Carrier?*, FINDLAW, http://injury.findlaw.com/torts-and-personal-injuries/what-is-a-common-carrier.html (last visited Oct. 1, 2015).

109. U.S. DEP'T OF JUSTICE, *Title III Highlights*, ADA.GOV, http://www.ada.gov/t3hilght.htm (last visited Oct. 1, 2015).

110. *Fact Sheet*, SELF STORAGE ASS'N, http://www.selfstorage.org/ssa/Content/NavigationMenu/AboutSSA/Factsheet/default.htm (last visited Oct. 1, 2015). About 10.85 million households in the United States rent a self-storage unit. *Id.*

111. *See 2014 U.S. Car Rental Market: Fleet, Locations and Revenue*, AUTO RENTAL NEWS, http://www.autorentalnews.com/fileviewer/2014.aspx (last visited Oct. 1, 2015).

112. *See* U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS iii (March 2007), *available at* http://www.justice.gov/oig/special/s0703a/final.pdf [hereinafter U.S. DOJ REVIEW OF § 215].

113. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L.

new clause authorized the FBI to apply for an order from FISC "requiring the production of *any tangible things* (including books, records, papers, documents, and other items)."[114] This meant that the government could acquire *any* record—be it business or personal.[115]

Congress also eliminated the restrictions on the types of commercial entities that could be served with an order.[116] Instead of just common carriers, public accommodation facilities, storage facilities, and vehicle rental facilities, orders could now be served on Internet service providers, grocery stores, libraries, booksellers, hotels, universities, and pharmacies—almost any institution or company.[117] The Department of Justice quickly interpreted this to mean any company with a domestic office, as well as any data in the company's "possession, custody, or control," even if it was stored overseas.[118]

The legislation, in addition, eliminated the requirement that the government demonstrate "specific and articulable facts" to the court that the target was a foreign power or an agent of a foreign power.[119] To the contrary, it only required that the person seeking the information state the "records concerned are sought for an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities."[120] Once the government provided its assurance, FISC became bound to grant the order.[121] By eliminating the link between the records and the target of the investigation, the government could collect information about *other* people, not personally suspected of any wrongdoing, as long as it related to an

No. 107-56, § 215, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861 (2012)); U.S. DOJ REVIEW OF § 215, *supra* note 112, at iii–iv.

114. Pub. L. No. 107-56, § 215, 115 Stat. at 287 (emphasis added).

115. *See id.*

116. *Compare* Pub. L. No. 107-56, § 215, 115 Stat. at 287, *with* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 602, 112 Stat. 2396, 2411–12 (codified as amended at 50 U.S.C. § 1861–1862 (2012)).

117. *See* Pub. L. No. 107-56, § 215, 115 Stat. at; U.S. D.O.J. REVIEW OF § 215, *supra* note 112, at 7.

118. *See* Cindy Cohn & Katitza Rodriguez, *Department of Justice Misdirection on Cloud Computing and Privacy*, EFF (Jan. 24, 2012), https://www.eff.org/deeplinks/2012/01/department-justice-misdirection-cloud-computing-and-privacy.

119. *Compare* Pub. L. No. 107-56, § 215, 115 Stat. at 287, *with* Pub. L. No. 105-272, § 602, 112 Stat. at 2411–12, *and* U.S. DOJ REVIEW OF § 215, *supra* note 112, at 8.

120. Pub. L. No. 107-56, § 215, 115 Stat. at 287–88.

121. *Id.*

authorized investigation.[122]

The government filed its first application for a tangible things order in May 2004.[123] That year, DOJ obtained seven orders.[124] In February 2005, it began using the authority in conjunction with pen register or trap and trace orders to obtain telephone subscriber information.[125] In 2005, the court issued 141 of the combination orders.[126] The types of information obtained included driver's license records, hotel records, apartment leases, credit card records, and subscriber information.[127]

The pressure to harvest social intelligence pushed the government past the statutory language that governed the acquisition of business records.[128] For the government to obtain an order, it must have "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment)."[129] The word "relevant" played a crucial role. The government's contention, which the Foreign Intelligence Surveillance Court eventually accepted, was that *all* metadata was potentially relevant to investigations.[130] Therefore, the government

122. *See id.*

123. U.S. DOJ REVIEW OF § 215, *supra* note 112, at 17.

124. *Id.*

125. *Id.* at 35.

126. *Id.*

127. *Id.* at 67. The DOJ was quick to say that it had not obtained library or bookstore records, medical records, or gun sale records. *See* Press Release, U.S. Dep't of Justice, Attorney General Alberto R. Gonzales Calls on Congress to Renew Vital Provisions of the USA PATRIOT Act, JUSTICE.GOV (April 5, 2005), *available at* http://fas.org/irp/news/2005/04/doj040505.html.

128. For a more detailed exposition of this point, see Donohue, *Metadata Collection*, *supra* note 16, at 802. *See also* Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 821 (2d Cir. 2015); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 171–72 (2014) [hereinafter PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, 215 REPORT] (agreeing in conclusion). *But see generally* DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (Jan. 19, 2006), *available at* https://epic.org/privacy/terrorism/fisa/doj11906wp.pdf (arguing legal justifications for the NSA program).

129. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106, 120 Stat. 192, 196 (codified as amended at 50 U.S.C. § 1861(b)(2)(A) (2012)).

130. *See, e.g.*, *In re* Application of the Fed. Bureau of Investigation for an Order

could collect all records.[131]

The error in this logic is clear. Specifically, why would Congress bother to use the word "relevant" if *all* records are relevant? That is, under this interpretation, nothing would be *ir*relevant. And it would not just be telephony metadata that the government could obtain under the government's interpretation, but all records, such as those related to banking or finance, education, and consumer purchases.[132]

The government's statutory interpretation similarly read the "reasonable grounds" requirement in the law out of existence.[133] If all records were relevant, then there would be no further limitation to only certain records for which it was reasonable to think that they related to the collection regime.[134] At the same time, the government's interpretation treated investigations as a class—not as a *particular* investigation already under way, as required by statute.[135] Further, the government collected information as part of a threat assessment—which was explicitly forbidden by statute.[136]

The program ran counter to other aspects of the statute as well. The legislation required, for instance, that the government be able to otherwise obtain the tangible goods being sought via subpoena duces tecum.[137] A prosecutor, however, would not be able to convene a grand jury and to begin collecting telephony metadata, just to see if there was any illegal activity afoot [138] The Supreme Court has explicitly ruled that subpoenas may not be used for fishing expeditions.[139]

Requiring the Prod. of Tangible Things, No. BR 15-75, at 14 (FISA Ct. 2015), *available at* http://www.fisc.uscourts.gov/sites/default/files/BR%2015-75%20Misc%2015-01%20Opinion%20and%20Order_0.pdf.

131. *See id.*

132. Donohue, *Metadata Collection*, *supra* note 16, at 841.

133. *Id.*

134. *Id.*

135. *Id.* at 849.

136. *Id.* at 846–47.

137. 50 U.S.C. § 1861(c)(2)(D) (2012).

138. *See In re* Grand Jury Subpoena Duces Tecum, 846 F. Supp. 11, 13 (S.D.N.Y. 1994).

139. United States v. R. Enters., Inc., 498 U.S. 292, 299 (1991) ("Grand juries are not licensed to engage in arbitrary fishing expeditions, nor may they select targets of investigation out of malice or an intent to harass.").

The telephony metadata program eviscerated the provisions of the statute that laid out what was required for installation and use of pen register or trap and trace devices.[140] The former is a "device or process which records or decodes dialing, routing, addressing, or signaling information"—i.e., the numbers dialed by a telephone.[141] The latter "captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information."[142] That portion of FISA also allows the government to obtain other, related information.[143] It must first, though, make a particularized showing in relation to the target about whom the information is going to be collected.[144] A judicial decision must be made *prior* to collecting information ,[145] and heightened protections are given to U.S. persons.[146]

By using the business records provision to obtain the same information—without any evidence of a connection to a foreign power or particularized showing of wrongdoing—the government performed an end-run around other statutory provisions.[147]

Despite the statutory violations, the NSA secretly collected telephony metadata in bulk.[148] The argument it offered to the FISC was that it was necessary to do this for national security purposes.[149] Both secretly and in the public debate that later ensued, the government offered a haystack rationale: it was necessary to build a haystack to find individuals who posed a threat.[150] In this case, the haystack was constructed of social relationships, the inspection of which might provide a clue to threats to U.S. national

140. *See* 50 U.S.C. §§ 1841–1846.

141. 18 U.S.C. § 3127(3).

142. *Id.* § 3127(4).

143. *See* 50 U.S.C. § 1842(a)(1)–(2).

144. *See id.* § 1842(d)(2)(A).

145. *See id.* § 1842(d)(1)–(2).

146. *Id.* § 1842(c)(2).

147. *See id.* § 1842(a)(2) (noting the authority under § 1842 is in addition to the authority to conduct electronic surveillance under FISA).

148. *In re* Production of Tangible Things from (Redacted), No. BR 08-13, at 1–2 (FISA Ct. Mar. 2, 2009), *available at* https://www.eff.org/document/br-08-13-order-3-2-09-final-redactedex-ocr-0.

149. *Id.* at 2.

150. *See* Scott Neuman, *Bush-Era NSA Chief Defends PRISM, Phone Metadata Collection*, NPR (June 09, 2013), www.npr.org/sections/thetwo-way/2013/06/09/190092800/bush-era-nsa-chief-defends-prism-phone-meta-data-collection.

security. It was the structure itself that had to be constructed to generate information.[151]

B. *Additional Social Intelligence Programs*

In June 2015 Congress responded to the public furor that accompanied the revelation that the intelligence community had been collecting Americans' telephone records by giving the government 180 days to end bulk telephony collection under Section 215.[152] This program, however, is only one of myriad ways in which the government is attempting to assimilate Big Data to reveal deeper insights into the social fabric.[153]

Starting in October 2001, President Bush operated a surveillance program entirely outside any statutory structure. Stellarwind collected telephone and Internet metadata, as well as telephone and Internet content.[154] It was so secret, that for the first few years, the NSA itself was not

151. *See id.*

152. *See* USA Freedom Act of 2015, Pub. L. No. 114-23, §§ 103, 109, 129 Stat. 268, 272, 276 (giving the government 180 days to end bulk collection of telephone records).

153. Also note, the Section 215 telephony metadata program accounts for only 41 orders issued under Section 215, leaving 711 orders, still classified, potentially untouched. *See* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE (forthcoming 2016). Additional telephony metadata programs exist. In January 2015, for instance, the DEA announced that it had been collecting telephony metadata between the United States and up to 116 different countries—in this case, apparently without *any* statutory authorization. Brad Heath, *U.S. Secretly Tracked Billions of Calls for Decades*, USA TODAY (Apr. 8, 2015), http://www.usatoday.com/story/news/2015/04/07/dea-bulk-telephone-surveillance-operation/70808616/.

154. President George W. Bush, Memorandum, Authorization for Specified Electronic Surveillance Activities During a Limited Period to Detect and Prevent Acts of Terrorism Within the United States (Oct. 4, 2001), *cited in* Office of the Inspector General, National Security Agency Central Security Service, ST-09-0002 Working Draft 1, 17–18 (2009), *available at* http://perma.cc/M3FC- QMHN. The Administration has publicly confirmed the inclusion of Internet and telephony metadata, and telephony content, as part of the program, but not Internet content. *See* Press Release, Director of National Intelligence, DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001 (Dec. 21, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,2001;
Unclassified Declaration of Frances J. Fleisch, National Security Agency, Jewel v. Nat'l Sec. Agency, No. 08-cv-4373-JSW (N.D. Cal. Dec. 20, 2013) [hereinafter Fleisch Declaration], *available at* https://www.eff.org/files/2013/12/21/fleisch2013jewelshubert

allowed to read the Office of Legal Counsel's (OLC) assessment of the legal grounds for the program, which had been provided to the President and Vice President.[155] At that time, some of the attorneys at OLC had an anomalous view of executive power—positions that OLC has since repudiated.

When questions were raised question about the legality and constitutionality of portions of Stellarwind, a concerted effort was made to force the collection of massive amounts of data into the existing FISA framework. The Internet metadata program was transferred to portions of the statute governing pen register and trap and trace devices.[156] It did so by reading "relevant" in the same way that it later interpreted Section 215,[157] stretching the meaning of the statutory language beyond common sense. Although the Internet metadata collection program formally ended in December 2011,[158] international Internet metadata collection appears to have continued through a program called "EVIL OLIVE."[159]

To incorporate the collection of other social network data into FISA's framing, the government re-defined "facility" to mean not a particular

.pdf (using language identical to DNI press release); *see also* Second Redacted Declaration of Steven G. Bradbury, Elec. Priv. Info. Ctr. v. Dep't of Justice, 511 F. Supp. 2d 56 (D.D.C. 2007) (No. 06-00214 HHK)), *available at* https://www.aclu.org/sites/default/files/pdfs/safefree/aclu_v_doj_2nd_declaration_steven_bradbury.pdf. For further discussion of these programs, see DONOHUE, *supra* note 153; SAVAGE, POWER WARS, *supra* note 16.

155. SAVAGE, POWER WARS, *supra* note 16, at 184.

156. *See* Foreign Intelligence Surveillance Court Memorandum Opinion (Redacted), 6 (FISA Ct.), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf; *see also* Foreign Intelligence Surveillance Court Opinion and Order (Redacted), 2 (FISA Ct.), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf (original order); *see also* 50 USC §§1841–1846; Press Release, Dir. of National Intelligence, DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After Attacks of September 11, 2001 (Dec. 21, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/991-dni-announces-the-declassification-of-the-exisitence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11,%202001.

157. *See* FISC Order, *supra* note 156, at 29–31; *see also* Donohue, *Metadata Collection*, *supra* note 16, at 836–38; SAVAGE, POWER WARS, *supra* note 16, at 197.

158. *See* DONOHUE, *supra* note 153.

159. Glenn Greenwald & Spencer Ackerman, *How the NSA is Still Harvesting Your Online Data*, THE GUARDIAN (June 27, 2013), http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

phone number or email address, but an entire gateway or cable head,[160] even as it transformed the meaning of "target" from relating to a particular individual, to entire groups, organizations, or networks.[161] This last alteration meant that the government could use the roving wiretap provisions inserted into FISA post-9/11 to wiretap any phone number or email address without first approaching the court.[162]

Other efforts to collect social intelligence have occurred under Modern FISA. As aforementioned, in 2008, the Administration convinced Congress to pass the FAA to give it more flexibility to intercept international traffic.[163] Section 702 of this statute allows the government to collect electronic communications on U.S. soil, where the target of the communications is not known to be a U.S. citizen and is believed to be located outside the United States.[164]

Leaked documents suggest that the government has used this provision to engage in programmatic collection, gaining insight into citizens' private relationships.[165] According to the Director of National Intelligence, only one order has been issued under the section, naming 89,138 targets.[166] When

160. SAVAGE, POWER WARS, *supra* note 16, at 201–202.

161. *Id.* at 205–206.

162. *Id.*; *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 206, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861 (2012)) (roving wiretap provision).

163. *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438; *See also* Donohue*, International Content, supra* note 18.

164. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, §702, 122 Stat. 2436, 2438. Under this provision, the Attorney General and the Director of National Intelligence may jointly authorize surveillance for up to one year. *Id.* at § 702(a). The statute prohibits the NSA from conducting reverse-targeting (i.e., targeting someone outside the U.S. with the purpose of collecting the communications of a specific person inside the U.S.). *Id.* at § 702(b)(2). It prohibits the collection of entirely domestic communications. *Id.* at § 702(b)(4).

165. *See, e.g.*, NSA, Exhibit B: Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (2009), *available at* http://perma.cc/F226-ASQ3; James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for U.S. Citizens' Emails and Phone Calls*, THE GUARDIAN (Aug. 9, 2013), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls.

166. OFFICE OF DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY

communications have one person based overseas (known as "one end foreign" or "1EF"), communications to or from the United States with that entity can be collected.[167] The NSA interprets the law to mean that it may not just collect information to or from the named targets, but any communications "about" the targets.[168] So, if two people who have no relationship to the target happen to mention the target, or "selectors" associated with the target, then their communications are identified and collected. In order to find out who is mentioning the target, or selectors associated with the target, the NSA must monitor all communications—with the result that Americans' international communications are subject to surveillance.

Two programs in the public domain are currently associated with Section 702. The first, PRISM, draws from Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL, and Apple—some of the largest communications providers, making the type of information that can be obtained substantial: email, video and voice chat, videos, photos, stored data, VoIP, file transfers, video conferencing, social networking details, and the like.[169]

REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013 (2014), *available at* http://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.

167. *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, §702, 122 Stat. 2436; *see also* Donohue*, International Content*, *supra* note 18.

168. *See* NSA, 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 (2009), *available at* http://perma.cc/E2NG-PU9P ("[I]n those cases where NSA seeks to acquire communications about the target that are not to or from the target, NSA will either employ an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas, or it will target Internet links that terminate in a foreign country."); *see also* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 38 (2014) [hereinafter PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., 702 REPORT], *available at* http://www.pclob.gov/Library/702-Report-2.pdf; Donohue*, International Content*, *supra* note 18, at 159.

169. Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-

The second, "upstream" collection under Section 702, amounts to collection from the servers of U.S. service providers.[170] It allows the NSA to acquire Internet communications "as they transit the 'internet backbone' facilities."[171] It monitors all traffic crossing cables—not just information targeted at specific Internet protocol addresses or telephone numbers.[172] By 2011, the NSA was acquiring around 26.5 million Internet transactions per year through upstream collection.[173]

While the full scope of social network collection outside of FISA is not publicly known, documents leaked over the past two years show that massive amounts of data are being obtained under Executive Order 12333. Under one program (Mystic), the NSA collects metadata on all mobile communications to, from, and within the Bahamas, Mexico, Kenya, the Philippines, and elsewhere.[174] In some cases, the NSA also collects the content of all telephone calls to, from, and within entire countries.[175] A

d970ccb04497_story.html; Glen Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data. The Privacy and Civil Liberties Oversight Board later clarified, "Once foreign intelligence acquisition has been authorized under Section 702, the government sends written directives to electronic communication service providers compelling their assistance in the acquisition of communications." PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., 702 REPORT, *supra* note 168, at 7.

170. *See* Foreign Intelligence Surveillance Court Memorandum Opinion (Redacted), (FISA Ct. Sept. 2012) [hereinafter FISC Mem. Op. 2012], *available at* https://www.aclu.org/files/assets/september_2012_fisc_opinion_and_order.pdf; Brett Max Kaufman, *A Guide to What We Now Know About the NSA's Dragnet Searches of Your Communications*, ACLU (Aug. 9, 2013), https://www.aclu.org/blog/guide-what-we-now-know-about-nsas-dragnet-searches-your-communications.

171. FISC Mem. Op. 2012, *supra* note 170170, at 26, https://www.aclu.org/files/assets/september_2012_fisc_opinion_and_order.pdf.

172. *See id.* at 26–27.

173. Foreign Intelligence Surveillance Court Memorandum Opinion and Order, 2011 WL 10945618, at *26 (FISA Ct. 2011).

174. Ryan Devereaux, Glenn Greenwald & Laura Poitras, *Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas*, THE INTERCEPT (May 19, 2014), https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.

175. *Id.*; *see also* Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls,* WASH. POST (Mar. 18, 2014), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

leaked NSA document notes that one such program processes over 100 million calls per day.[176]

The data being collected includes email address books and contact lists, which can be analyzed to build robust social models. In conjunction with the NSA's UK counterpart, General Communication Headquarters (GCHQ), for example, the government appears to be tapping Yahoo and Google's internal networks to harvest address books and instant messaging contact lists, implicating hundreds of millions of customers.[177]

According to a leaked, internal NSA slide presentation, in a single day in 2012, NSA's Special Source Operations branch collected nearly half a million address books from Yahoo, more than 100,000 from Hotmail, approximately 82,000 from Facebook, another 33,000 from Gmail, and some 23,000 from other providers.[178] Muscular, as the program is called, holds the information in a temporary buffer, where it is scanned for certain information.[179] Data considered relevant is then sent back to the NSA.[180] The volume is considerable: between December 2012 and January 2013, more than 181 million new records were obtained in this way.[181]

Webcam images and chat sessions are also appear to be collected under Executive Order 12333. GCHQ files from 2008 to 2010 reference a program called Optic Nerve, in which Yahoo webcam chats were collected in bulk, regardless of whether the individual user was a foreign intelligence target.[182] During one six-month period, GCHQ, with the help of the NSA, collected visual data from more than 1.8 million Yahoo user accounts around the

176. Devereaux, Greenwald & Poitras, *supra* note 174.174

177. Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

178. *Id.*

179. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

180. *Id.*

181. *Id.*

182. Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, THE GUARDIAN (Feb 28, 2014), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

world.[183] The system began as an experiment in automated facial recognition, with one image every five minutes selected from users' feeds.[184] Access to all Yahoo webcam images or events provided the agencies with insight into online users.[185] The information was then fed into NSA's XKeyscore search tool.[186]

Text messages similarly are not immune. In 2011, an internal slide presentation at the NSA referred to SMS Text Messages "A Goldmine to Exploit."[187] Under Executive Order 12333, the NSA has collected almost 200 million text messages per day, globally, using them to ascertain location, travel plans, social networks, and credit card details.[188] Like the bulk collection of telephony metadata under Section 215 of the USA PATRIOT Act, the SMS message program, codenamed Dishfire, is not targeted.[189]

In addition to direct text messages, the program provides the government with access to missed-call alerts, which can be used to conduct contact-chaining analysis, to determine international movement (e.g., from network roaming alerts), or to obtain electronic business cards, financial transactions, or geolocation data from requests by people for route information or to set up meetings.[190]

The NSA also collects geolocational information. Nearly 5 billion records per day help the agency to find mobile phones around the world, and to map relationships between mobile telephone users.[191] By some accounts,

183. *Id.* As a domestic matter, there are no restrictions on the NSA's collection of information on British subjects, just as there are no British restrictions on GCHQ's collection of information on American citizens. *Id.*

184. *Id.*

185. *Id.*

186. *Id.* Private, sexually explicit webcam material proved to be a particular challenge: between 3 percent and 11 percent of the Yahoo webcam imagery obtained by GCHQ contained "undesirable nudity." *Id.*

187. *See NSA Dishfire Presentation on Text Message Collection—Key Extracts*, THE GUARDIAN (Jan. 16, 2014), http://www.theguardian.com/world/interactive/2014/jan/16/nsa-dishfire-text-messages-documents.

188. James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep*, THE GUARDIAN (Jan. 16, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep; *see also Dishfire Presentation*, *supra* note 187.

189. Ball, *supra* note 188; *see also Dishfire Presentation*, *supra* note 187.

190. Ball, *supra* note 188.

191. Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013),

the agency has more than 27 terabytes of data associated with this program.[192]

The NSA has constructed databases to house this social network information. XKeyscore appears to have the widest-reaching collection of online information.[193] It includes Digital Network Intelligence—understood as "nearly everything a typical user does on the internet," such as email, social media, chats, websites visited, and metadata.[194] The amount of information is staggering. William Binney, a former mathematician at the NSA, said in 2012 that, looking solely at phone calls and emails, the agency had "assembled on the order of 20 trillion transactions about U.S. citizens with other U.S. citizens."[195] At some sites, the amount of data obtained daily is so massive (more than 20 terabytes), that it can only be stored for short periods.[196]

These programs signal the dawn of a new age of intelligence collection—one centered on the acquisition and analysis of digitized information about social relationships. Significant risks attend.

IV. THE DANGERS OF SOCIAL NETWORK ANALYSIS

Social network construction and analysis can reveal our most intimate details.[197] Social intelligence derives, in part, from the type of information at issue in the telephony metadata program.[198] In many ways, such data is more devastating than pure content.

As Stewart Baker, NSA's former general counsel, stated,, "Metadata

http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

192. *Id.*; *see also FASCIA: The NSA's Huge Trove of Location Records*, WASH. POST, http://apps.washingtonpost.com/g/page/world/what-is-fascia/637 (last visited Nov. 2, 2015).

193. Greenwald, *XKeyscore*, *supra* note 30.

194. *Id.*

195. Glenn Greenwald, *Are All Telephone Calls Recorded and Accessible to the US Government?*, THE GUARDIAN (May 4, 2013), http://www.theguardian.com/commentisfree/2013/may/04/telephone-calls-recorded-fbi-boston.

196. Greenwald, *XKeyscore*, *supra* note 30.

197. *See Written Testimony of Edward W. Felten, United States Senate, Committee on the Judiciary Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act*, 113th Cong. 7–8 (2013) [hereinafter *Written Testimony*].

198. Mayer & Mutchler, *supra* note 62.

absolutely tells you everything about somebody's life."[199] Baker concluded, "If you have enough metadata you don't really need content . . . . [It's] sort of embarrassing how predictable we are as human beings."[200] General Michael Hayden concurred, stating Baker was "absolutely correct."[201] Hayden added, "We kill people based on metadata."[202]

Even if citizens want to prevent their metadata from being collected, it would be almost impossible to do so.[203] Encryption is advancing; however, most of its trajectory centers on protecting content—not metadata.[204] The only realistic option therefore is to refrain from using digital technology.[205] Doing so, however, would mean rejecting the contemporary world, with potentially devastating consequences for one's relationships, employment, and personal affairs.[206]

Metadata matters because it offers reliable information about a broad range of behavior, offering insight into what we have done, as well as what we are likely to do.[207] Social media does the same, as does pattern analysis

199. Alan Rusbridger, *The Snowden Leaks and the Public*, N.Y. REV. BOOKS (Nov. 21, 2013), http://www.nybooks.com/articles/archives/2013/nov/21/snowden-leaks-and-public/.

200. *Id.* (alteration in original).

201. David Cole, *'We Kill People Based on Metadata,'* N.Y. REV. BOOKS (May 10, 2014), http://www.nybooks.com/blogs/nyrblog/2014/may/10/we-kill-people-based-metadata/.

202. *Id.* For a discussion of the use of telephony metadata in signature strikes (predator drone strikes based on SIGINT and patterns of behavior), see Dana Priest, *NSA Growth Fueled by Need to Target Terrorists*, WASH. POST (July 21, 2013), http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html; Jeremy Scahill & Glenn Greenwald, *NSA's Secret Role in the U.S. Assassination Program,* THE INTERCEPT (Feb. 9, 2014), https://firstlook.org/theintercept/2014/02/10/the-nsas-secret-role/.

203. Donohue, *Metadata Collection*, *supra* note 16, at 874; Decl. of Prof. Edward Felton at ¶¶ 30–37, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-cv-03994), *available at* https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf.

204. Donohue, *Metadata Collection*, *supra* note 16, at 874.

205. *Id.*

206. *Id.*

207. *See, e.g.*, Decl. of Prof. Edward Felton, *supra* note 203, at 58; Klayman v. Obama, 957 F. Supp. 2d 1, 18–19 (D.D.C. 2013), *vacated and remanded*, No. 14-5004, 2015 WL 5058403 (D.C. Cir. Aug. 28, 2015); Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 730 (S.D.N.Y. 2013).

based on movement. A tremendous amount of information can be conveyed, in the process creating vulnerabilities.

A. *What Analytics Can Demonstrate*

Even seemingly innocuous data, like the telephony metadata at issue in the Section 215 program, can carry with it deep implications for individual privacy. A study conducted in 2015 by computer scientists at Stanford University determined that "phone metadata is unambiguously sensitive," even when collected for three months on just over 500 people.[208] The researchers were able to attribute a range of medical conditions and beliefs to the participants in the study, based solely on telephony metadata.[209] Calls to health services, financial services, pharmacies, sexually transmitted disease clinics, divorce lawyers, strip clubs, recruiting and job placement organizations, and religious organizations—even alone—provide inferential information about a person.[210]

Patterns in the numbers dialed and received reveal even more.[211] One person in the Stanford study talked to cardiologists, then telephoned a medical laboratory, after which the subject received calls from a pharmacy, and later telephoned a cardiac arrhythmia device home reporting hotline.[212] Another person called a firearms store known for selling AR-15 semiautomatic rifles, prior to calling a gun manufacturer's customer service.[213] Another subject contacted a home improvement store, a locksmith, a dealer for hydroponics, and a head shop.[214] A fourth person talked for a considerable amount of time to her sister.[215] Forty-eight hours later, she telephoned Planned Parenthood.[216] Two weeks afterwards, she called the clinic a few times, and a month later called one last time.[217]

The metadata represented a small sample, over a short period, with a limited number of calls. Nevertheless, it revealed participants' heart

208. Mayer & Mutchler, *supra* note 62.
209. *Id.*
210. *Id.*
211. *Id.*
212. *Id.*
213. *Id.*
214. *Id.*
215. *Id.*
216. *Id.*
217. *Id.*

conditions, gun purchases, cannabis cultivation, and decision to have an abortion.[218]

The collection of Internet and telephony metadata allows the government to engage in social network analysis, building a detailed picture of citizens' connectedness to each other—of what types of issues matter to us—and of our stature in the social fabric.[219] The ability to do so relates to the rapid growth of new technologies and scholarly fields.[220] Digital platforms have created the potential for mass communication.[221] The Internet distributes worldwide communications at the speed of light. In light of these advances, publications centered on social network analytics have exponentially accelerated.[222] "[S]everal hundred papers in physics, mathematics, computer science, biology, economics, and sociology"[223] and numerous books, have put forward new theories and algorithms contributing to the evolution of network science.[224] Powerful advances in computing, such as the advent of the cloud industry, which gives users access to supercomputers around the globe and the ability to process information, mean that massive datasets can now be built and mined to generate new knowledge.[225] More details about social behavior can be learned.[226]

These technologies are so strong that they may produce information that individuals do not even know about themselves. They may not know

218. *Id.*

219. *See Written Testimony*, *supra* not207e 197, at 10–11.

220. *See* DAVID KNOKE & SONG YANG, SOCIAL NETWORK ANALYSIS 2 (2d ed. 2008).

221. *See, e.g.*, Nagehan Ilhan, Sule Gündüz-Ögüdücü, & A. Sima Etaner-Uyar, *Introduction to Social Networks: Analysis and Case Studies*, *in* SOCIAL NETWORKS: ANALYSIS AND CASE STUDIES 1, 2 (2014).

222. *Id.*

223. Duncan J. Watts, *The "New" Science of Networks,* 30 ANN. REV. SOC. 243, 243–44 (2004).

224. JOHN SCOTT, SOCIAL NETWORK ANALYSIS 1–2 (3d ed. 2013); For a discussion on social network analysis and related areas, see Ilhan, Günduz-Ögüdücü, & Etaner-Uyar, *supra* note 221, at 1–2; N. Gizen Kocak, *Social Networks and Social Network Analysis*, 5 INT'L J. BUS. & SOC. SCI. 126, 126 (2014); Réka Albert and Albert-László Barabási, *Statistical Mechanics of Complex Networks,* 74 REVIEWS OF MODERN PHYSICS 47, (2002) (reviewing recent advances in the field of complex networks).

225. *See, e.g.*, Ilhan, Günduz-Ögüdücü, & Etaner-Uyar, *supra* note 221, at 14–16; Ruxandra-Ştefania Petre, *Data Mining in Cloud Computing*, 3 DATABASE SYSTEMS J. 67, 67–68 (2012), *available at* http://www.dbjournal.ro/archive/9/9_7.pdf.

226. Mayer & Mutchler, *supra* note 62.

how important they are in the formal and informal groups of which they are a part. But this can now be measured. A variable called "centrality" can be calculated to ascertain their relative worth and to provide insight into how influential they may be.[227] There are different ways in which centrality can be measured.[228] How short the paths are between people, how many links they have to others, and how close they are to other potentially powerful people in the network provide insight into how much power they wield—and how they may exercise it.[229] Structural cohesion generates insight.[230]

People may not realize their own habits, or the seriousness with which they view certain issues, but both may become clear by the frequency with which they act on their interests and beliefs. They may not know how dependent they are on certain relationships. They may not be aware of the degree of power that others have over them, or that they have over others. They may not have insight into connections between those with whom they are linked and others, or how closely others, with whom they are connected, are tied into groups whose interests they oppose or do not share.[231] They may be unaware that some of those who are in their group of associates are only in contact with them for instrumental reasons, using the relationship to secure goods, services, or information for purposes that are masked from their view. They may not be able to see others, virtual strangers to them, who have a significant amount of power over their activities and their ability to pursue their interests, simply because of these strangers' centrality in networks of which all are a part.[232]

Social network analytics allow people to find patterns in relations that evolve over time.[233] Analysis may focus on individuals, small groups, organizations, or even entire countries.[234] When all Internet or telephony metadata is collected, the unit under consideration could be any number, or configuration of individuals.[235]

227. Ilhan, Günduz-Ögüdücü, & Etaner-Uyar, *supra* note 221, at 4.

228. *See id.* at 5–7.

229. *See id.*

230. *Id.* at 6.

231. The academic literature refers to this as "boundary penetration relations," where individuals may be members of two or more social formations. *See* KNOKE & YANG, *supra* note 220, at 12.

232. *See, e.g.*, KNOKE & YANG, *supra* note 220, at 4.

233. *Id.* at 2.

234. *Id.*

235. *See id.*

The basic idea is that the regular patterns of relations between different points provide a macrosocial context—or overall structure—which, in turn, influences individuals' precepts, beliefs, decisions, and actions.[236] As one scholar explains: "The central objectives of network analysis are to measure and represent these structural relations accurately, and to explain both why they occur and . . . their consequences."[237] Structure matters more than an individual's age, gender, or ideology.[238] It reveals how powerful individuals may be in ways that may not otherwise be obvious.[239] A woman holding a menial job that does not require a significant amount of initiative may be a strong member of the neighborhood organization or the parent-teacher association.[240] Social network analysis provides insight into how social status and strength—even of the same person—may vary across contexts.[241]

Social network analytics carry with them a tremendous amount of power.[242] If one political party accesses the telephone records of the opposing party, it can identify the most powerful actors and then find a way either to alter their behavior or to separate them from the network.[243] Doing so could disrupt political opposition. It could be done in quite visible ways, such as finding evidence of illegal behavior and initiating prosecution against the target—or in less visible ways, such as pressuring the surrounding network to get the target to act in a certain way.

B. *What Analytics Can Do*

One of the insights discovered by social science is that relationships with others influence perceptions, beliefs, and actions.[244] The stronger the connection with others, or the more intense the interaction with them, the more susceptible people are to their influence.[245] As a result, identifying high

236. *Id.* at 4.
237. *Id.*
238. *Id.*
239. *See id.* at 5.
240. *Id.*
241. *Id.* at 9.
242. *Id.* at 116.
243. *See, e.g.*, Steve Ressler, *Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research*, HOMELAND SEC. AFF. 1, 2 (July 2006), *available at* https://www.hsaj.org/articles/171.
244. KNOKE & YANG, *supra* note 220, at 4; *see also* Duncan, J. Watts, *supra* note 223, at 256.
245. *See* Florence Passy, *Social Networks Matter*, *But How?*, *in* SOCIAL MOVEMENTS

intensity relationships offers a lever to change others' behavior.[246]

Behavior modification can be done not just for one person, but for a series of individuals with a high level of centrality in social networks. Those who control such corridors, or pathways, can put themselves in a position of social (or political) control.[247] The scholarly literature is full of examples of how controlling structural relations generates competitive, or cooperative, behavior—whether it is in political movements, drug trafficking networks, terrorist campaigns, or even regular corporate environments.[248]

The power of social networks to affect political change has already been demonstrated in the Philippines, Spain, Tunisia, Egypt, and elsewhere.[249] Concerted development or study of social networks as a *prelude* to action opens a new door of vulnerability. The government can use social networks to force political, economic, and social change. The U.S. has already conducted programs, based on SOCINT, to try to build and then to influence the powerful nodes in social networks.[250] The aim of the enterprise was to counter political opposition to the United States.[251]

In 2010 the U.S. government created a "Twitter" to generate a social

AND NETWORKS: RELATIONAL APPROACHES TO COLLECTIVE ACTION 21, 33 (Mario Diani & Doug McAdam eds., 2003).

246. *See* Ramkrishnan V. Tenkasi & Marshal C. Chesmore, *Social Networks and Planned Organizational Change: The Impact of Strong Ties on Effective Change Implementation and Use*, 39 J. APPLIED BEHAV. SCI. 281, 283 (2003).

247. *Id.*

248. *See, e.g.,* MARC SAGEMAN, UNDERSTANDING TERROR NETWORKS 137 (2004) (Al Qaeda and the Salafi jihad); Phil Williams, *Transnational Criminal Networks*, *in* NETWORKS AND NETWARS 61, 61 (John Arquilla & David Ronfeldt, eds., 2001) (criminal organizations); Richard M. Medina, *Social Network Analysis: A Case Study of the Islamist Terrorist Network*, 27 SECURITY J. 97, 97–99 (2014) (Islamist terrorism); Passy, *supra* note 245, at 33 (social/political movements); Jörg Raab & H. Brinton Milward, *Dark Networks as Problems*, 13(4) J. PUB. ADMIN. RES. & THEORY 413, 420–28 (2003) (drug-trafficking, the Al Qaeda network, diamond and weapons trade); Ressler, *supra* note 243, at 2 (terrorist networks); Tenksai & Chesmore, *supra* note 246, at 290 (multinational corporations).

249. *See supra* Part II.

250. Associated Press, *U.S. Secretly Created "Cuban Twitter" to Stir Unrest and Undermine Government*, THE GUARDIAN (Apr. 3, 2014) [hereinafter AP, *Cuban Twitter*], http://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest.

251. *See id.* (describing that the goal of the program was to "undermin[e] Cuba's communist government" and that the program was ran by an office whose goal was to promote U.S. interests).

network in Cuba that could then be manipulated to undermine the government.[252] The Associated Press, which reported on the project, reviewed more than 1,000 pages of documentation and conducted multiple interviews with people involved.[253] It found that it was not the CIA behind the initiative, but USAID, a development agency—not even a formal part of the intelligence community structure.[254]

The program was called ZunZuneo, which is slang in Cuban for the noise made by a hummingbird.[255] It began by "tweeting" soccer results, music, and weather reports—all rather benign.[256] Once ZunZuneo reached a critical mass of Cuban subscribers, though, the plan was to begin inserting content that would create "smart mobs," which could be mobilized at will, to trigger a "Cuban spring."[257] The purpose of the program was to "renegotiate the balance of power between the state and society."[258]

USAID went to great lengths to mask the role of the U.S. government—including from Congress itself.[259] The legislature had become increasingly concerned about the agency's Office of Transition Initiatives, which it stood up just after the fall of the Soviet Union to promote U.S. interests abroad.[260] Staff Members of the Senate Foreign Relations recount how they could not even find out in broad terms what USAID was doing.[261] Senator Patrick Leahy, Chair of the Appropriations Committee's State Department and Foreign Operations subcommittee did not know about the program—even though his subcommittee ostensibly had oversight of it.[262]

USAID similarly tried to infiltrate the underground hip-hop scene in Cuba, to spark a youth movement to overthrow President Raul Castro.[263]

252. *Id.*
253. *See id.*
254. *See id.*
255. *Id.*
256. *Id.*
257. *Id.*
258. *Id.* (quotation marks omitted).
259. *See id.*
260. *Id.*
261. *Id.*
262. *See id.*; *see also* Associated Press, *Senate Committee Probes "Cuban Twitter" USAid ZunZuneo Programme*, THE GUARDIAN (Apr. 10, 2014) [hereinafter AP, *ZunZuneo*], http://www.theguardian.com/world/2014/apr/10/senate-committee-cuban-twitter-usaid-zunzuneo.
263. Matthew Weaver & Associated Press, *US Agency Infiltrated Cuban Hip-hop*

These initiatives were done secretly, without Congressional oversight—and billed not as covert action, but as an attempt to build civil society in Cuba.[264] The purpose was to gain social and political control.[265]

The collection of SOCINT offers the government a rich opportunity to leverage the information because social networks are not static.[266] They are continually evolving.[267] Therefore, they can be used to manipulate and to alter individual and organizational behavior.[268] They offer insight into specific attributes—such as what individuals like, or do not like, to do—as well as relations between people and groups, and characteristics of the type of connectedness in question.[269] What is the nature of the relationship between two people? Trust? Advice? Support? Or betrayal? Social network analytics provide a context for relationships.[270]

Since 9/11, much attention has been paid to how to use network analysis to respond to threats to U.S. national security.[271] One conclusion that researches have reached is that it is difficult to obtain information about highly secretive, global organizations that make it a point not to post data on otherwise publicly available sites.[272] But networks of all kinds have to

Scene to Spark Youth Unrest, THE GUARDIAN (Dec. 10, 2014), http://www.theguardian.com/world/2014/dec/11/cuban-hip-hop-scene-infiltrated-us-information-youth.

264. *See* AP, *ZunZuneo*, *supra* note 262.

265. *See id.*

266. *See* Ressler, *supra* note 243, at 1–3.

267. *Id.*

268. *See, e.g.*, Patrick Kenis & David Knoke, *How Organizational Field Networks Shape Interorganizational Tie-Formation Rates,* ACAD. OF MGMT. REV. 275, 277 (2002).

269. *See* Ilhan, Günduz-Ögüdücü, & Etaner-Uyar, *supra* note 221, at 1.

270. *See id.*

271. *See* Ressler, *supra* note 243, at 3 ("After the attacks of 9/11, academia, the government, and even mainstream media began to discuss the importance of social network analysis in fighting terrorism.").

272. Valdis E. Krebs, *Mapping Networks of Terrorist Cells*, 24(3) CONNECTIONS 43, 44, 56 (2002), *available at* http://insna.org/PDF/Connections/v24/2001_I-3-7.pdf; Malcolm K. Sparrow, *The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects*, 13 SOC. NETWORKS 251, 262 (1991) (discussing the incompleteness of criminal network data); *see also* Kathleen Carley, *Estimating Vulnerabilities in Large Covert Networks*, *in* PROCEEDINGS OF THE 2004 INTERNATIONAL SYMPOSIUM ON COMMAND AND CONTROL RESEARCH AND TECHNOLOGY 2 (Carnegie-Melon Univ. June, 2004); Matthew Dombroski, Paul Fischbeck & Kathleen M. Carley, *Estimating the Shape of Covert Networks*, *in* PROCEEDINGS OF THE 8TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM 2 (National

communicate—after all, that is what makes them a network—and global communication systems analytics offer one way forward. Thus, we find ourselves in an age of social intelligence.

There are numerous difficulties with this approach. First, in some ways, it has not been particularly effective.[273] While the government initially claimed that the telephony metadata program was a critical part of discovering and thwarting dozens of planned attacks, after Congressional scrutiny, only one instance could be produced where the government had used the Section 215 program to identify a terrorist.[274] Basaaly Moalin, a cab driver in San Diego, donated money to al-Shabab in Somalia.[275] Even this

Defense War College, Washington, DC, 2003); Maksim Tsvetovat & Kathleen Carley, *On Effectiveness of Wiretap Programs in Mapping Social Networks* 1 (2006), *available at* http://www.cs.rit.edu/~amt/linkanalysis06/accepted/23.pdf. *But see* Center for Computational Analysis of Social and Organizational Systems, *Networks and Terrorism CASOS Projects*, CASOS, http://www.casos.cs.cmu.edu/terrorism/projects.php (last visited Oct. 5, 2015) (using complex modeling to analyze covert networks by relying on predictive modeling of network structure).

273. *See, e.g.*, Peter Bergen, *NSA and Your Phone Records*: *What Should Obama Do*?, CNN (Jan. 15, 2014), http://www.cnn.com/2014/01/15/opinion/bergen-nsa-obama-phone/.

274. Mattathias Schwartz, *The Whole Haystack: The N.S.A. Claims it Needs Access to All Our Phone Records. But is That the Best Way to Catch a Terrorist?*, THE NEW YORKER, (January 26, 2015), http://www.newyorker.com/magazine/2015/01/26/whole-haystack ("[A]s evidence of the fifty-four disrupted plots came apart, many people in Washington shifted their rhetoric on Section 215 away from specific cases and toward hypotheticals and analogies."). Initial claims by the Government conflated Section 702 and Section 215 data and were later found to be overblown. For example, General Keith Alexander stated before Congress that "the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world." Bergen, *supra* note 273 (quotation marks omitted). Representative Mike Rogers, chair of the House Permanent Select Committee on Intelligence, claimed in July 2014 that "54 times the NSA programs 'stopped and thwarted terrorist attacks both here and in Europe—saving real lives." *Id.* Senator Patrick Leahy subsequently attacked these numbers, noting that they conflated the content collection programs with the metadata collection programs. *Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs: Hearing Before the Sen. Judiciary Comm.*, 113th Cong. 1–3 (2013) (statement of Sen. Patrick Leahy, Chairman) *available at* http://fas.org/irp/congress/2013_hr/fisa-oversight.pdf.

275. Ellen Nakashima, *NSA Cites Case as Success of Phone Data-Collection Program*, WASH. POST (Aug. 8, 2013), https://www.washingtonpost.com/world/national-security/nsa-cites-case-as-success-of-phone-data-collection-program/2013/08/08/fc915e5a-feda-11e2-96a8-d3b921c0924a_story.html ("Across a dozen years of records collection, critics say, the government has offered few instances in which the massive

example was weak: for two months after discovering Moalin's complicity in terrorist actions overseas, the FBI declined to take any further action.[276]

Scholars and experts have looked into the question and concluded that, as a means of uncovering terrorist plots, communications metadata, in particular, is full of weaknesses.[277] In 2008, the National Research Council of the Academies of Science released the results of an intensive study conducted by prominent academics in computer science, data mining, behavioral science, terrorism, and law.[278] "Modern data collection and analysis techniques," the final report stated, "have had remarkable success in solving information-related problems in the commercial sector. . . . But such highly automated tools and techniques cannot be easily applied to the much more difficult problem of detecting and preempting a terrorist attack, and success in doing so may not be possible at all."[279] The Privacy and Civil Liberties Oversight Board (PCLOB), after looking carefully at the NSA's telephony metadata program, similarly determined that it "has not proven useful in identifying unknown terrorists or terrorist plots."[280] To the contrary, information obtained through querying the metadata merely confirmed relationships that had already been determined through other means.[281] Weighed against the government's potential use of the information for myriad purposes, the PCLOB called for an end to the program.[282]

The lack of effectiveness of bulk collection of metadata has been echoed by a number of studies. The New America Foundation, for instance, analyzed 225 individuals recruited by al Qaeda and similar organizations and subsequently charged with terrorism.[283] "Traditional investigative methods,

storehouse of Americans' records contained the first crucial lead that cracked a case — and even those, they say, could have been obtained through a less intrusive method."); *see also* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., 702 REPORT, *supra* note 168.

276. Nakashima, *supra* note 275.

277. *See, e.g.*, NATIONAL RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 2–3 (2008).

278. *Id.* at 1–2.

279. *Id.* at 2.

280. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., 215 REPORT *supra* note 128, at 158.

281. *Id.*

282. *Id.*

283. Bailey Cahall et al., *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, NEW AMERICA (Jan. 13, 2014), https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/.

such as the use of informants, tips from local communities, and targeted intelligence operations, provided the initial [identification of the individuals]," even as the bulk collection program provided minimal help.[284] "Indeed, the controversial bulk collection of American telephone metadata," the Foundation explained, "appears to have played an identifiable role in initiating, at most, 1.8 percent of these cases."[285]

One possible reason that metadata may not be effective for counterterrorism stems from the "snowballing" method adopted by the government.[286] Agents identify a particular telephone number, find associated numbers, and then determine the numbers to which those numbers are linked. The problem is that this approach is biased towards highly connected networks.[287] Terrorist organizations, however, commonly work along a cell structure, in which there are relatively weak connections between actors.[288] It is not the *most* connected that are likely to engage in terrorist activity, but those on the periphery that are more likely to be involved in violence.[289] A similar claim has been made about Islamist networks—that they are sparsely populated and structured along a cell system.[290]

A second, important consideration is that every person in the United States relies on communications networks to go about their daily lives. It would be difficult to live in the contemporary world without a telephone or access to the Internet. And so, it is not just potential terrorists' metadata that is collected (and for which such a method is significantly flawed), but all Americans' data. Citizens find their most intimate lives exposed to the government.[291] Unlike Islamist organizations, which often have sparse communication networks and, because of their structure, are not as vulnerable to social network analytics, ordinary citizens' social networks may be extremely dense, generating much more—and more intimate—information.[292] The cost is borne by individual liberty and inroads into

284. *Id.*
285. *Id.*
286. *See* Tsvetovat & Carley, *supra* note 272, at 1–2.
287. *Id.* at 15–16.
288. *Id.* at 2.
289. *Id.*
290. *See* Medina, *supra* note 248, at 101.
291. *See* Donohue, *Metadata Collection*, *supra* note 16, at 759–60
292. *See id.* at 871–72.

privacy.

V. FOURTH AMENDMENT PRINCIPLES

While the technological capabilities of social network mapping are revolutionary, the concerns that accompany the growth of the field are far from new. The Founders introduced the Fourth Amendment to protect against the danger that the government could cast about for information, which it could then use to bring criminal charges.[293] The Founders were deeply concerned about the potential harms caused by allowing the government access to citizens' private lives. Doing so threatened solitude, intimate relations, and even democratic deliberation. It was too much power to put into one place. In taking the position that they did, the Founders drew heavily from their English legacy.[294]

A. *Prohibition on General Warrants*

A general warrant is a document, issued by a court or by the executive branch, giving officials the broad authority to search for and to seize private documents, without any prior, specific evidence of wrongdoing.[295] It does not specify, with particularity, the person or place to be searched, or the papers or records to be seized.[296] It is not supported by oath or affirmation of any wrongdoing.[297]

For hundreds of years prior to the founding, English jurists considered general warrants to be a violation of the British Constitution.[298] Thus it was that Sir Edward Coke insisted in Parliament that the Petition of Right

293. *See generally* Laura K. Donohue, *The Original Fourth Amendment*, U. CHI. L. REV. (forthcoming 2016) [hereinafter Donohue, *The Original Fourth Amendment*] (discussing, in detail, the historical origins of the Fourth Amendment and its rejection of General Warrants); *see also* William Cuddihy & B. Carmon Hardy, *A Man's House Was Not His Castle: Origins of the Fourth Amendment to the United States Constitution*, 37 WM. & MARY Q. 371, 372 (1980).

294. Donohue, *The Original Fourth Amendment*, *supra* note 293, (manuscript at 28); Cuddihy & Hardy, *supra* note 293, at 372.

295. Donohue, *The Original Fourth Amendment*, *supra* note 293; Cuddihy & Hardy, *supra* note 293, at 372; *see also* William C. Banks, *A Look at the Global Response to Terrorism: The Death of FISA*, 91 MINN. L. REV. 1209, 1209–11 (2007).

296. *See* Donohue, *The Original Fourth Amendment*, *supra* note 293.

297. Thomas Y. Davies, *Recovering the Original Fourth Amendment,* 98 MICH. L. REV. 547, 550–51 (1999).

298. *Id.*

include a clause prohibiting promiscuous search and seizure.[299] It was against the Reason of the Common Law (and thus "unreasonable") to allow for such instruments. No royal prerogative, or reason of state, could justify such tyrannical instruments:

> [I]f [imprisonment] be *per mandatum domini regis*, or 'for matter of state'; and then we are gone, and we are in a worse case than ever. If we agree to this imprisonment 'for matters of state' and 'a convenient time,' we shall leave Magna Carta and the other statutes and make them fruitless, and do what our ancestors would never do.[300]

Coke returned to these arguments in his *Institutes of the Laws of England*, writing that to issue a general warrant is against Magna Carta.[301]

In 1678, Sir Matthew Hale similarly condemned general warrants in the first volume of his *Pleas of the Crown: or, A Methodical Summary of the Principal Matters Relating to that Subject*.[302] Later, in *Historia Placitorum Coronæ* (History of the Pleas of the Crown), Hale wrote, "[A] general warrant to search in all suspected places is not good, but only to search in such particular places, where the party assigns before the justice his suspicion and the probable cause thereof, for these warrants are judicial acts, and must be granted upon examination of the fact."[303]

It was to Hale's writing that Lord Chief Justice Mansfield famously appealed in the case of *Money v. Leach*.[304] In other cases, such as *Entick v. Carrington* and *Wilkes v. Wood*, the English law lords repeatedly rejected general warrants.[305] Similarly, it was to Coke and Hale that Serjeant-at-Law

299. Coke to Parliament, Committee of the Whole House, Proceedings and Debates, ff. 100–100v, in CD, III, 149–51 (Apr. 29, 1628) *reprinted in* THE SELECTED WRITINGS OF SIR EDWARD COKE, at 1270–71.

300. Coke to Parliament, Committee of the Whole House, Proceedings and Debates, f. 99, in CD, III, 94–96(Apr. 26, 1628), *in* SELECTED WRITINGS, *supra* note 299, at 1268.

301. EDWARD COKE, THE THIRD PART OF THE INSTITUTES OF THE LAWS OF ENGLAND 35 (1644) ("*Nec super eum ibimus, nec super eum mittimus, nisi per legale judicium parium suorum, vel per legem Terrae* [Neither will we pass upon him, or condemn him, but by the lawful judgment of his peers, or by the law of the land].").

302. *See* SIR MATTHEW HALE, PLEAS OF THE CROWN, A METHODICAL SUMMARY OF THE PRINCIPAL MATTERS RELATING TO THAT SUBJECT 93 (1678) (citing C. Jur. Courts, p. 177).

303. 2 SIR MATTHEW HALE, HISTORIA PLACITORUM CORONÆ 150 (1736).

304. Money v. Leach, (1765) 97 Eng. Rep. 1075 (K.B.) 1083, 1088.

305. Entick v. Carrington, (1976) 19 How. St. Tr. 1029 (C.P.) 1072–73; Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (C.P.) 490.

William Hawkins appealed in his *Pleas of the Crown* to state the illegality of general warrants: "I do not find any good Authority, That a Justice can justify sending a general Warrant to search all suspected Houses in general for stolen Goods."[306] Probable cause must first be demonstrated (under oath), particularity attached, and a specific warrant issued.[307] A number of influential English legal treatises and abridgements followed Hawkins's *Pleas*, condemning general warrants.[308]

By the time of the founding, William Blackstone's *Commentaries on the Laws of England* announced that the question had been well settled:

> Sir Edward Coke indeed has laid it down that a justice of the peace cannot issue a warrant to apprehend a felon upon bare suspicion; no, not even till an indictment be actually found: and the contrary practice is by others held to be grounded rather upon connivance than the express rule of law; though now by long custom established.[309]

For Blackstone, "A *general* warrant to apprehend all persons suspected, without naming or particularly describing any person in special, is illegal and void for its uncertainty; for it is the duty of the magistrate, and ought not to be left to the officer, to judge of the ground of suspicion."[310]

The rejection of general warrants traversed the Atlantic. When the Crown tried to make greater use of promiscuous search and seizure to crack down on smuggling, colonists rejected the practice as contrary to their rights as Englishmen.[311]

James Otis's speech challenging the Crown's use of general warrants is one of the most famous orations in U.S. history.[312] More than five decades

306. 2 WILLIAM HAWKINS, PLEAS OF THE CROWN 84 (1716–1721).

307. *Id.* at 82, 84.

308. *See, e.g.*, 4 RICHARD BURN, THE JUSTICE OF THE PEACE, AND THE PARISH OFFICER 105–07 (12th ed. 1772).

309. 4 WILLIAM BLACKSTONE, COMMENTARIES *290 (1769).

310. *Id.* at 291 (citing HALE, *supra* note 302, at 580; HAWKINS, *supra* note 306, at 82).

311. *See, e.g.*, Circular from William Pitt to Francis Bernard (Aug. 23, 1760), *in* THE PAPERS OF FRANCIS BERNARD: GOVERNOR OF COLONIAL MASSACHUSETTS, 1760–1769, at 52–53 (Colin Nicolson ed., 2007) [hereinafter Circular from William Pitt]; JOSIAH QUINCY, JR., REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY BETWEEN 1761 AND 1772, at 407–08 (Samuel M. Quincy ed., 1865); *see also* Donohue, *The Original Fourth Amendment*, *supra* note 293.

312. *See id.*

afterwards, John Adams, who had been present at the time, related, "Otis was a flame of fire!"[313] His performance had "breathed into this nation the breath of life."[314] Adams declared, "Then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."[315]

Otis attacked the idea that the government could simply collect information to try to find evidence of wrongdoing: "I will to my dying day oppose with all the powers and faculties God has given me, all such instruments of slavery on the one hand, and villainy on the other, as this writ of assistance is."[316] The writ of assistance was "the worst instrument of arbitrary power, the most destructive of English liberty and the fundamental principles of law, that ever was found in an English law-book."[317]

The writs created the potential for misuse of the power for personal purposes.[318] Otis lamented, "Every man, prompted by revenge, ill humor, or wantonness, to inspect the inside of his neighbor's house, may get a writ of assistance. Others will ask it from self-defence; one arbitrary exertion will provoke another, until society be involved in tumult and blood."[319] Otis echoed Coke: the Reason of the Common Law demanded that the Court find such instruments illegal.[320]

The colonists' rejection of general warrants did not end with the founding. In Virginia, Patrick Henry, George Washington, Edmund Pendleton, George Mason, George Wythe, Richard Henry Lee, and Thomas Jefferson, among others, adopted a provision in the Virginia Declaration of Rights condemning general warrants.[321] In Pennsylvania, Benjamin Franklin, George Bryan, James Cannon, Thomas Paine, and others did the same.[322] The newly formed states of Delaware, Maryland, North Carolina,

313. *Id.* (quotation marks omitted).
314. *Id.* (quotation marks omitted).
315. *Id.* at 248.
316. 2 JOHN ADAMS, THE WORKS OF JOHN ADAMS 523 (Charles F. Adams ed., 1865).
317. *Id.*
318. *See id.* at 524–25.
319. *Id.*
320. *See id.*
321. *See* VA. CONST. art. I, § 10; *Delegates to the Constitutional Convention: Virginia*, UM-KC, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/marryvirginia.html (last visited Oct. 5, 2015).
322. *See* PA. CONST. art. I, § 10 (1776); *Delegates to the Constitutional Convention: Pennsylvania*, UM-KC, http://law2.umkc.edu/faculty/projects/ftrials/conlaw/marrypenn.

Massachusetts, Vermont, and New Hampshire all banned general warrants.[323]

Early Americans repeatedly articulated the right to be secure against unreasonable search and seizure as the grounds on which general warrants would not be allowed.[324] As Adams wrote in the Massachusetts document, "Every subject has a right to be secure from all unreasonable searches and seizures of his person, his houses, his papers, and all his possessions."[325]

"Unreasonable" here had a particular meaning: namely, against reason or opposed to common law.[326] General warrants violated the common law.[327] The Massachusetts Constitution continued,

> All warrants, *therefore*, are contrary to this right, if the cause or foundation of them be not previously supported by oath or affirmation; and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the persons or objects of search, arrest, or seizure . . . .[328]

By using "therefore" in this way, Adams underscored that it was to ensure the right against unreasonable search and seizure, that general warrants, and special warrants lacking an oath, evidence, and particularity with regard to the persons to be arrested or places to be searched, would not be allowed.[329] The state constitution added, "[A]nd no warrant ought to be issued but in cases, and with the formalities prescribed by the laws."[330] Only warrants that comported with the requisite particularity, supported by oath, would be valid.[331] These state declarations transformed the colonists' objection to general warrants into a positive right.[332]

---

html (last visited Oct. 5, 2015).

323. *See* DEL. CONST. art. I, § 17; MD. CONST. art. I, § 23; N.H. CONST. of 1784 Pt. I, art. XIX; N.C. CONST. art. I, § 11; VT. CONST. art. I, § 11.

324. *See, e.g.*, *supra* note 275 & accompanying text.

325. MASS. CONST. of 1780, pt. I, art. XIV.

326. *See* Donohue, *The Original Fourth Amendment*, *supra* note 293.

327. *See id.*

328. MASS. CONST. of 1780, pt. I, art. XIV (emphasis added).

329. *See id.*

330. *Id.*

331. *See id.*

332. *See, e.g.*, *supra* note 325 & accompanying text; MASS. CONST. of 1780, pt. 1, art. XIV.

In 1787, the new constitution transformed federal power.[333] The ratification debates immediately seized on whether a prohibition on general warrants would be required to protect individual rights.[334] In Virginia, Patrick Henry demanded that a bill of rights be adopted to preserve the rights and privileges of the people.[335] He worried that government officials could go into citizens "cellars and rooms, and search, ransack, and measure every thing you eat, drink, and wear."[336] "I feel myself distressed," he admitted,

> because the necessity of securing our *personal rights* seems not to have pervaded the minds of men; for many other valuable things are omitted. For instance, general warrants, by which an officer may search suspected places, without evidence of the commission of a fact . . . .[337]

Property could be taken "in the most arbitrary manner, without any evidence or reason."[338] Everything considered sacred could "be searched and ransacked by the strong hand of power."[339] Delegates agreed.[340] Virginia proposed that a bill of rights, which included a prohibition on general warrants, be adopted.[341]

In New York, a "Son of Liberty" predicted that general warrants would be one of the curses that would "be entailed on the people of America, by this preposterous and newfangled system, if they are ever so infatuated as to receive it."[342] According to the writer, "Men of all ranks and conditions, subject to have their houses searched by officers, acting under the sanction of *general warrants*, their private papers seized, and themselves dragged to prison, under various pretences, whenever the fear of their lordly masters

333. *See Constitution of the United States—A History*, NATIONAL ARCHIVES, http://www.archives.gov/exhibits/charters/constitution_history.html (last visited Oct. 5, 2015).

334. *See, e.g.*, 3 THE DEBATES IN THE SEVERAL STATE CONVENTIONS: ON THE ADOPTION OF THE FEDERAL CONSTITUTION 468, 658 (Jonathan Elliot ed., 2d ed. 1901).

335. *Id.* at 593–94.

336. *Id.* at 414.

337. *Id.* at 532.

338. *Id.*

339. *Id.*

340. *Id.* at 657.

341. *Id.*

342. *A Son of Liberty*, NEW YORK JOURNAL, Nov. 8, 1787, *reprinted in* 1 VOLUME XIX, RATIFICATION BY THE STATE: NEW YORK 134, 134 (2009), *available at* http://csac.history.wisc.edu/son_of_liberty.pdf.

shall suggest, that they are plotting mischief against their arbitrary conduct."[343]

The New York convention went so far as to insist that it was *only* with the understanding that Congress would amend the Constitution to take account of the right against general search, and others laid out in its ratification document, that it consented to the new Constitution.[344] The convention attached a military reservation to make it clear that it did not make its representation lightly.[345]

Rhode Island, Maryland, Massachusetts, and Pennsylvania followed suit.[346] In the last, Samuel Bryan, an Anti-Federalist writing as "Centinel," repeatedly raised a similar concern.[347] He wrote, "Your present frame of government secures you to a right to hold yourselves, houses, papers and possessions free from search and seizure."[348] Bryan explained, "therefore warrants granted without oaths or affirmations first made, affording sufficient foundation for them . . . shall not be granted."[349] The right against promiscuous search and seizure hung in the balance: "whether your *papers*, your *persons*, and your *property*, are to be held sacred and free from *general warrants*, you are now to determine."[350] Madison incorporated these concerns into what is now the Fourth Amendment.[351]

The collection of SOCINT raises constitutional concerns in the extent to which it results in private information being collected by the government

343. *Id.* (emphasis in original).

344. *See* 1 THE DEBATES IN THE SEVERAL STATE CONVENTIONS: ON THE ADOPTION OF THE FEDERAL CONSTITUTION 329, 329 (Jonathan Elliot ed., 2d ed. 1891).

345. *Id.* ("In full confidence, nevertheless, that, until a convention shall be called and convened for proposing amendment to the said Constitution, the militia of this state will not be continued in service out of this state for a longer term than six weeks, without the consent of the legislature thereof.").

346. *See id.* at 319–20, 323–25, 335.

347. *To Thomas Jefferson from Samuel Brian*, NATIONAL ARCHIVES, http://founders.archives.gov/documents/Jefferson/01-33-02-0069 (last visited Oct. 5, 2015).

348. Centinel, No. 1, (Oct. 5, 1787), *reprinted in* THE COMPLETE BILL OF RIGHTS: THE DRAFTS, DEBATES, SOURCES, AND ORIGINS 349 (Neil H. Cogan ed., 2d ed. 2015).

349. *Id.*

350. *Id.* (emphasis in original).

351. *See* Thomas Y. Davies, *Correcting Search-and-Seizure History: Now-Forgotten Common-Law Warrantless Arrest Standards and the Original Understanding of "Due Process Law*,*"* 77 MISS. L.J. 1, 138–39 (2007).

without evidence of prior wrongdoing.[352] Nor do the SOCINT programs underway specify the individual about whom information is to be obtained; instead, information is generally collected about everyone, with the hope of uncovering illegal activity. That this information is now being queried using U.S. person information, for criminal matters unrelated to foreign intelligence collection, further underscores the deep constitutional questions at stake.

It was precisely to prevent the government from collecting massive amounts of information that the Founders adopted the Fourth Amendment.[353] They were concerned about the potential use of such information for political purposes—to head off opposition to the government, or to the government's political, social, or economic agenda.[354] One of the dangers they perceived was precisely that at issue in the ZunZuneo case: that the information could be used for political purposes.[355]

New and emerging technologies magnify the Founders' concerns. Not only could the collection of private information cause great mischief, but the digitization of so much information has also deepened privacy interests.[356] It is not just the details about an individual with whom one is in correspondence, but the details of *everyone* with whom citizens communicate, their degree of power in different networks, and the strength of their relationships with other people and entities.[357]

In the post-Snowden era, one example of SOCINT that has gained

352. *See generally* Donohue, *The Original Fourth Amendment*, *supra* note 293 (discussing the history of general warrants); *see also* Donohue, *Metadata Collection*, *supra* note 16, at 863–65 (2014); Klayman v. Obama, 957 F. Supp. 2d 1, 37 (D.D.C. 2013) (declining to answer the question of whether the collection of metadata violated the Fourth Amendment, but noting it is "significantly likely" such collection does violate the protections of the Constitution), *vacated and remanded*, No. 14-5004, 2015 WL 5058403, at *9 (D.C. Cir. Aug. 28, 2015).

353. *See* Rand Paul & Chris Coons, *The Founding Fathers Would Have Protected Your Smartphone*, POLITICO (May 27, 2014), www.politico.com/magazine/story/2014/05/a-tech-challenge-for-fourth-amendment-application-107129.

354. *See id.*

355. *See* AP, *Cuban Twitter*, *supra* note 250.

356. *See* Mayer & Mutchler, *supra* note 62 (discussing sensitive and even criminal inferences that can be from metadata).

357. *See id*; *see also* Ilhan, Günduz-Ögüdücü, & Etaner-Uyar, *supra* note 221, at 1–3.

prominence among scholars revolves around Paul Revere.[358] What, exactly, was his role in the Revolution? It turns out that he was more than just a messenger.[359] Using the membership rosters of Whig groups, social network scholars have demonstrated that Revere was a key link between revolutionary entities, spanning different social strata and connecting disparate organizations.[360] As such, he played a central role in forging the movement.[361] As Shin-Kap Han, a Professor of Sociology at the University of Illinois at Urbana-Champaign, pointed out, the key question was not who Revere was, but how and why he mattered to the underlying structure and, in turn, to the outcome of the movement.[362] When mapped, Revere's centrality to the Revolution becomes clear.

In 1776, the British Government did not have access to the types of digital information and algorithmic analytics that today mark the field.[363] Whether an individual was involved in the St. Andrews Lodge, the Loyal Nine, the North Caucus, the Long Room Club, the Tea Party, or the Boston Committee, might have been available on a limited bases because of HUMINT.[364] The social network analytics that would have given this information deeper meaning, though, had yet to be constructed.[365]

Some commentators have pointed to the Revere data as evidence for why SOCINT ought to be collected.[366] The Revolutionists, after all, were engaged in a violent upheaval against the government.[367] Others see the potential as precisely the type of government overreach that justified the

358. Shin-Kap Han, *The Other Ride of Paul Revere: the Brokerage Role in the Making of the American Revolution*, 14 MOBILIZATION: AN INT'L Q. 143, 143–62 (2009), *available at* http://www.sscnet.ucla.edu/polisci/faculty/chwe/ps269/han.pdf; Kieran Healy, *Using Metadata to Find Paul Revere* (Jun. 9, 2013), http://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/.

359. Han, *supra* note 358, at 143.

360. *Id.*

361. *Id.*

362. *Id.*

363. *See* Healy, *supra* note 358.

364. *See id.*

365. *See id.*

366. *See, e.g.*, Joshua Brustein, *What if the 'Redcoat NSA' Had Access to Paul Revere's Metadata?* BLOOMBERG (June 12, 2013), http://www.bloomberg.com/bw/articles/2013-06-12/what-if-the-redcoat-nsa-had-access-to-paul-reveres-metadata.

367. Sean Hollister, *Paul Revere Could Have Been Caught if the British Crown Collected Metadata*, THE VERGE (Jan. 17, 2014), http://www.theverge.com/2014/1/17/5319534/paul-revere.

Revolution in the first place.[368]

Whatever one's take on the data might be, at a minimum, it is clear that SOCINT offers an incredibly powerful tool—one that is qualitatively different from other forms of intelligence, and one that carries with it the potential for devastating harm. Equally important are the rights implications underlying the collection of such information in the first place.

B. *Protection of Individual Rights*

Not all information that contributes to SOCINT derives from communications metadata. Other information, such as that gleaned from social network sites, may be substantive.[369] Telephony metadata, however, provides a good case study because some see it as an outlier—as not implicating the same privacy interests as content.[370]

This argument is backed by Supreme Court doctrine dating back to the 1970s, when landlines dominated communications.[371] In *Smith v. Maryland*, the Court ruled that telephony data provided to third parties does not enjoy Fourth Amendment protections.[372]

The problems with this argument are manifold. Most concerning, it fails to acknowledge that the entire point of collecting social intelligence is to map relationships and levels of intimacy between individuals. The Founders, rightly, evinced concern about giving the government insight into citizens' private lives.[373]

Part of the reason for their aversion relates to the harms detailed above.[374] That is, the information could be used to blackmail individuals opposed to the rulers' social, political, or economic policies.[375] Information could be used to discredit others—or criminal charges for unrelated offenses could be introduced to prevent opposition.[376] The advent of SOCINT creates precisely the opportunity for such mischief. It was not the Founders' sole

368. *See id.*
369. *See* PATTON, *supra* note 15, at 12.
370. *See* Smith v. Maryland, 442 U.S. 735, 745 (1979).
371. *See id.*
372. *Id.*; Donohue, *Metadata Collection*, *supra* note 16, at 863–71.
373. *See* Paul & Coons, supra note 353.
374. *Id.*
375. *Id.*
376. *See* Mayer & Mutchler, *supra* note 62; AP, *Cuban Twitter*, *supra* note 250.

concern.

Early Americans also worried about rights themselves.[377] The walls of the home stood as a proxy for the right to privacy, the protection of which provided multiple benefits for self and society.[378] The right to guard against unwelcome intrusion meant that a safe haven could be created, within which individuals could retreat from the outside world.[379] Solitude, and the need to protect individuals against intrusion from others, becomes ever more important in the digital age. It is important because it allows individuals to develop autonomy and ideas.

By tracking social relationships, the government risks incursions into this private sphere. If individuals think they are being watched, their behavior changes.[380] This impacts our ability to develop our ideas, and it hurts intimacy between individuals.[381] Diversity in one's relationships, however, is an essential part of human development. It also matters for the strength of the social fabric.[382] If people fear the government tracking them because they are in conversations with individuals from an ethnic or religious group considered suspect, then the ties between individuals in that group and those outside that group may significantly weaken.[383] So, too, may relationships among group members dissipate. What results is a much weaker social fabric with long-term consequences for humanistic interests of each person, much less the social ties themselves. It is not just the right to privacy that is hurt by SOCINT, but also associated rights such as the right to free association and the right to free speech. One may not communicate with others because of fear of government intrusion, thus harming one's ability to articulate different beliefs, thoughts, and ideas.

There is yet another aspect of the right itself that affects the nature of the state, and that is democratic deliberation.[384] SOCINT makes it

377. *See* Donohue, *The Original Fourth Amendment*, *supra* note 293, (manuscript at 40–41); Cuddihy & Hardy, *supra* note 293, at 391–400.

378. *See* Donohue, *The Original Fourth Amendment*, *supra* note 293 (manuscript at 36); Cuddihy & Hardy, *supra* note 293, at 400.

379. *See* Donohue, *The Original Fourth Amendment*, *supra* note 293 (manuscript at 36); Cuddihy & Hardy, *supra* note 293, at 371–72.

380. *See, e.g.*, Linda E. Fisher, *Guilt by Expressive Association; Political Profiling, Surveillance and the Privacy of Groups*, 46 ARIZ. L. Rev. 621, 646 (2004).

381. *See id.* at 646–50.

382. *See id.*

383. *See id.*

384. *See* Donohue, *The Original Fourth Amendment*, *supra* note 293 (manuscript at

exceedingly easy to monitor political communities, which, as a result, may well alter their level of engagement with political or economic concerns. Surveillance therefore may harm society's ability to develop more robust policies, as well as stifle public debate about the strengths and weaknesses of the current regime.

A final consideration relates to structure itself. The intelligence agencies represent just one portion of one branch of the federal government.[385] This type of power, amassed in the hands of the few and ripe for abuse, has long term consequences for the distribution of power both among the federal branches of government as well as between the federal and state entities.[386]

VI. CONCLUDING REMARKS

Rapid technological and algorithmic advances have given rise to a new form of information: social intelligence. This tool, which centers on the collection of non-traditional forms of data about relationships, such as those offered by social media, communications data, and geolocational information, offers novel insights into the fabric of society. It provides a starting point for further socio-cultural knowledge generation. And it can be used to effect massive political, social, and economic change. As such, it qualitatively differs from other forms of intelligence.

The current statutory regime proves ill-fitting for the type of information involved. The government's attempted use of FISA to authorize telephony metadata collection fell far short of the statutory requirements. Nor did efforts to force Internet metadata into FISA's pen register and trap and trace provisions fare better. In the meantime, Modern FISA is being stretched to incorporate a wide range of social intelligence about U.S. citizens, even as Executive Order 12333 provides a broad framing for yet more collection of such sensitive information.

One problem is that SOCINT can be used for not just ascertaining threats to the United States but also for heading off political opposition.[387]

11–13).

385. *See Structure*, INTELLIGENCE.GOV, http://web.archive.org/web/20150628204228/http://www.intelligence.gov/mission/structure.html (last visited Oct. 5, 2015).

386. *See* Michael P. Noonan, *Defense Intelligence Agency Expansion Must Be Closely Monitored*, U.S. NEWS & WORLD REPORT (Dec. 5, 2012), www.usnews.com/opinion/blogs/world-report/2012/12/05/defense-intelligence-agency-expansion-must-be-closely-monitored.

387. *See, e.g.*, AP, *Cuban Twitter*, *supra* note 250.

Important nodes can be identified and neutralized, or pressured to act in certain ways. Social networks are also vulnerable to manipulation. They are dynamic processes and thus constantly changing and evolving. Information can be disseminated quickly among the members of the network. Because they lack a territorial grounding, and instead are formed through the digital sphere, networks evolve with scant regard for political borders or regulatory structures. Communication, moreover, may occur instantaneously between lots of people, bringing massive human resources to bear.

Another concern relates to the constitutional underpinning of the United States. The Fourth Amendment was created to protect against the broad collection of information on U.S. citizens because of the harms that could ensue.[388] SOCINT is a powerful type of data. Had the British had access to it at the time of the Revolution, a very different outcome may have ensued.[389] Whether one takes heart from this or despairs of it, the central point cannot be ignored: SOCINT carries with it an enormous amount of power. The rights basis also matters. The invasion of privacy may have deleterious consequences for values central to the United States.

Together, these considerations suggest that more careful discussion of SOCINT takes place, before it fully evolves—not least because of the unique challenges it poses as a matter of U.S. constitutional law. Traditional FISA currently addresses electronic communications, physical search, pen register and trap and trace devices, and tangible goods. For the most part, SOCINT is now being collected under Modern FISA and Executive Order 12333. The time is ripe for Congress to extract these programs from the current framing and to amend FISA directly to take account of the promise—and perils—of social intelligence.

388. *See supra* Part IV.

389. *See, e.g.*, Brustein, *supra* note 366.