American University Business Law Review

Volume 4 | Issue 1 Article 7

2014

Data Retention Requirements And Outsourced Analysis: Should Private Entities Become Government Surrogates In The Collection Of Intelligence?

Michael J. Woods

DATA RETENTION REQUIREMENTS AND OUTSOURCED ANALYSIS: SHOULD PRIVATE ENTITIES BECOME GOVERNMENT SURROGATES IN THE COLLECTION OF INTELLIGENCE?

MICHAEL J. WOODS*

Introduction 49
I. The President's Data Retention Proposal 50
II. Telephone Providers as Government Surrogates 54
Conclusion 60

INTRODUCTION

June 5, 2013 marked the beginning of an extraordinary, though not unprecedented, period in the history of the American intelligence community. Following extensive (and unauthorized) revelations of U.S. "bulk collection" programs targeting telephone metadata, both the Executive Branch and Congress have embarked on a more or less comprehensive review of intelligence activities and the intricate regulatory structure that is meant to restrain these activities within Constitutional parameters. In many aspects, the present experience is similar to the experience in 1974-1978, when aggressive investigative journalism brought to light the extent to which U.S. intelligence agencies were engaging in questionable activities, including largely unsupervised domestic surveillance operations. In the 1970s, these disclosures led to extensive Congressional investigations, the promulgation of Executive Orders governing the conduct of all intelligence activities, and the creation of a statutory framework to govern intelligence surveillance activities

* Michael J. Woods is a Vice President & Associate General Counsel of Verizon Communications Inc. He previously served as Counsel in the National Security Division in the U.S. Department of Justice; as Chief of the FBI's National Security Law Unit; and as Principal Legal Advisor at the National Counterintelligence Executive. The views expressed in this article are those of the author, and do not reflect the official policy or position of Verizon or any U.S. government component.

conducted within the United States.

The present instance of this reflective process, however, also introduces some significant new themes. In the 1970s, the clear impulse in response to the revealed abuses was to directly regulate government activity.[1] Though the intelligence reforms of the mid-1970s occurred when the reputations of Executive Branch institutions were at a historically low ebb, there appeared to be a consensus that those government institutions, fitted out with proper oversight, could safely conduct intelligence activities. In the post-Snowden reform discussions, this consensus is much less in evidence. It may be that the perceived inadequacies of the 1970s-era oversight structure in the face of post 9/11 pressures fatally undermined the belief that some combination of regulatory, judicial, and Congressional oversight can be sufficient to control intelligence agencies. In any case, reform discussions now include the consistent theme that the collection, searching, and perhaps even analysis of potentially relevant data is best done by the private holders of that data not the government.

My intention here is to briefly examine whether private entities should ever serve as government surrogates in the collection or analysis of data. Mindful of the limitations of writing while this topic is in "mid-discussion," I will first examine the current proposals, and the assumptions underlying those proposals. Then, I will explore some of the issues that, in my view, militate against the surrogacy and note trends in communications technology that ought to be addressed in any reform discussions.

I. THE PRESIDENT'S DATA RETENTION PROPOSAL

Within weeks of the first Snowden disclosures, President Obama commissioned a special review group to examine the issues surrounding "bulk collection" of data and to make policy recommendations to him.[2] Shortly thereafter, Congress requested that the pre-existing Privacy and Civil Liberties Oversight Board ("PCLOB") conduct an inquiry into the newly disclosed surveillance activities.[3] Both bodies consulted widely with

---

1. For a thorough description of the reform process, *see* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS at Chapter 2 (regulation of intelligence activities) and Chapter 3 (regulation of intelligence surveillance and searches, specifically). (2d ed. 2012).

2. *See* Memorandum Reviewing Our Global Signals Intelligence Collection and Communications Technologies, 2013 DAILY COMP. PRES. DOC. 567 (Aug. 12, 2013) *available at* http://www.gpo.gov/fdsys/pkg/DCPD-201300567/pdf/DCPD-20130056 7.pdf.

3. For the initial Congressional request, *see* Letter from Tom Udall et al., U.S. Senators, to the Privacy and Civil Liberties Oversight Board (June 12, 2013), *available at* http://www.pclob.gov/Library/Letter-Senate_letter_to_PCLOB-Jun2013.pdf. Additional members of Congress joined the request in subsequent days.

intelligence agencies, outside interest groups, academics, policymakers, and representatives of industry.

The Presidential review group, known formally as the Review Group on Intelligence and Communications Technologies, released its report on December 12, 2013.[4] The report contained numerous recommendations, but one that garnered particular attention was that bulk collection of telephony metadata might be replaced by a "system in which such metadata is held instead either by private providers or by a private third party."[5] Less than a month later, on January 14, 2014, President Obama announced his proposals to reform U.S. intelligence collection operations.[6] He issued a Presidential Decision Directive that made changes to the operational rules affecting intelligence collection.[7] He then announced, conditionally, the end of bulk collection of telephony metadata pursuant to Section 215 of the USA PATRIOT Act and appeared to endorse (though noted certain difficulties) the Review Group's recommendation on non-government entities holding the metadata.[8] The condition was important: his Administration, together with Congress, would work to come up with a solution that enabled the intelligence community to obtain the information it requires while leaving the metadata in the hands of the telephone companies.[9] The bulk collection program was to continue until the solution, which had an original due date of March 28, 2014, was fully in place.[10] The March 28 deadline passed, and the Administration announced that the

---

4. *See* THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

5. *Id.* at 25 (focusing on Recommendation number five).

6. Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 DAILY COMP. PRES. DOC. 30 (Jan. 17, 2014), *available at* http://www.gpo.gov/fdsys/pkg/DCPD-201400030/pdf/DCPD-201400030.pdf.

7. Press Release, The White House Office of the Press Sec'y, Presidential Policy Directive – Signals Intelligence Activities (Jan. 17, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

8. The collection in bulk of telephone metadata had been authorized under the "business records" section of the Foreign Intelligence Surveillance Act of 1978 ("FISA"), which is codified at 50 U.S.C. § 1861. This application of section 1861 was enabled by the expansion of the business records authority by section 215 of the USA PATRIOT Act. *See* 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 (2001). For this reason, the FISA business records provision is commonly known as "Section 215."

9. *See* Remarks on United States Signals Intelligence and Electronic Surveillance Programs, *supra* note 6, at 7.

10. *Id.*

bulk collection program would continue until the solution was enacted.[11] The PCLOB issued an extensive report on January 23, 2014, and, though consultation with the PCLOB was noted in the President's statement, it does not appear that the PCLOB findings were as closely linked to the Administration's policy as those of the Review Group.[12]

As of October 2014, the Administration has yet to release a detailed proposal for "solving" the bulk collection problem or any particular details regarding how the "data retention by provider" concept might be implemented. The implementation details are important, since there is no guarantee that the telephone companies will retain, or continue to maintain, metadata for a long enough period of time to satisfy the needs of the intelligence community. In the present system of bulk collection (at least as it has become publicly known) the government compels the major telephone carriers to turn over "call detail records" in bulk, perhaps on a daily basis.[13] The intelligence community then retains these records for a period of five years, and queries them as needed.[14] If this system transitions to one in which the telephone companies did not hand over records in bulk to the government, but rather, executed individualized queries against the stock of records that the company holds in the ordinary course of business, then the length of time that the company holds its own records becomes particularly relevant. [15] If, for example, the intelligence agency requires that records be searched five years into the past and the telephone companies only retain such records for twelve months, then

---

11. *See* Presidential Statement on the National Security Agency's Section 215 Bulk Telephony Metadata Program, 2014 DAILY COMP. PRES. DOC. 213 (Mar. 27, 2014), *available at* http://www.gpo.gov/fdsys/pkg/DCPD-201400213/pdf/DCPD-201400213.pdf (commenting that data "should remain at the telephone companies for the length of time that it currently does today.").

12. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., 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 168 (2014), *available at* http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf. Interestingly, the PCLOB explicitly rejected the idea of data retention by providers.

13. Declassified versions of the "primary order" issued by the Foreign Intelligence Surveillance Court ("FISC") indicate that two companies are compelled to produce records. *See* Primary Order, BR-14-01 (FISC January 3, 2014) at 3-4. Redacted version of order *available at*, http://www.fisc.uscourts.gov/sites/default/files/BR%2014-02%20Order-2.pdf.

14. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 12, at 21–37.

15. *See, e.g., United and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act:* ("USA FREEDOM Act"): *Hearing on H.R. 3361 Before the S. Select Comm. on Intelligence*, 113th Cong. (2014) (statement of Sen. Dianne Feinstein, Chairman, S. Select Comm. on Intelligence), *available at*, http://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=a6cbcb99-b19d-41a4-be93-ae4b98410dab.

either the agency will have to forego the ability to search beyond twelve months or the company will have to be compelled to retain its records for a longer period of time. This reasoning assumes, of course, that the intelligence agencies actually need access to historical records, and this is far from a settled question. Many, most notably the PCLOB, have questioned the examples cited as justification for the bulk telephony program.[16] The amount of time that metadata retains a demonstrable intelligence value appears to be a "soft" number at present, but there will need to be a consensus value for any solution to proceed.

The intelligence value question opens a very complex debate, even when that debate is restricted to just traditional telephony. Telephone companies retain call detail records as "business records," that is, records that are generated in the ordinary course of business and are retained for as long as needed in the conduct of the company's business.[17] The business need for call detail records has evolved over time. In the past, they were an essential component of the telephone billing systems relevant to most customers. As the billing function has transitioned, CDRs remain important for other business functions like traffic management and load balancing in the telephone networks, calculation of inter-company transactions between telephone providers, and fraud investigations. However, the retention periods associated with each of these functions may vary from one company to the next, and even between components of a single company (i.e. wireless networks vs. landline networks; international vs. domestic).[18]

How the President's proposal will craft a workable solution is likely to depend heavily on Congress. The current FISA statute contains no explicit provision at all for data retention, and thus, it is unlikely that the creation of such requirements is within the existing authority of the Foreign Intelligence Surveillance Court ("FISC"). The solution, therefore, will certainly require legislative action. There is no shortage of legislative proposals, but none so far have addressed the specific challenge of data retention. In general, the legislative proposals fall into three categories: (1)

---

16. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 12, at 145–155.

17. Some have suggested that the Federal Communications Commission regulations require telephone companies to retain call detail records for eighteen months. *See* 47 C.F.R. § 42.6 (2000). In fact, the FCC requirement is to retain certain customer billing records—which increasingly do not incorporate call detail records at all.

18. A generic description of these business uses is often included in the privacy policy statements of telephone companies. *Compare Privacy Policy Summary*, VERIZON WIRELESS, https://www.verizon.com/about/privacy/ (last updated Nov. 2013) *with AT&T Privacy Policy*, AT&T, http://www.att.com/gen/privacy-policy?pid=2506 (last visited Feb. 22, 2014).

those that focus on enhanced oversight of intelligence agency activity without substantially altering Section 215;[19] (2) those that simply abolish the ability to conduct bulk collection pursuant to Section 215;[20] and (3) those that abolish bulk collection, but provide a targeted alternative means for the intelligence community to obtain data from private entities.[21] Whether any of these develop into an option that meets the twin goals of the stated Administration policy (meeting intelligence needs but providers retaining the data), or whether the Administration's view prevails at all remains unknown. As the discussion intensifies, the data retention question likely will come back into focus, and the possibility of requiring companies to retain, or even analyze, data on the government's behalf will need serious examination.

II. TELEPHONE PROVIDERS AS GOVERNMENT SURROGATES

Lacking a specific proposal to critique, the next stage of my inquiry is to broadly examine the issues in a proposal that would require telephone companies to retain call detail records (or equivalent telephony metadata) for a period defined without reference to the use of those records in ordinary business. The companies would then be required to produce records in response to targeted queries authorized by the FISC Those queries could require the simple delivery of information, and might also require the provision of information prospectively or the production of records found to be associated with the queried numbers. Thus, the notional solution would require the telephone company both to retain data, and to produce the data in a specified format (perhaps entailing some rudimentary analysis of the data on the part of the company).

The foundational question here is whether or not such a data retention scheme better serves to protect Constitutional interests. There is a lively debate in the courts as to the Constitutional significance of the telephony metadata at issue in the bulk collection program.[22] Although difficult to

19. *See, e.g.*, FISA Improvements Act of 2013, S. 1631, 113th Cong. (as reported by S. Comm. on Intelligence, Oct. 31, 2013) (enhances oversight and reporting requirements but retains ability to conduct bulk collection under Section 215).

20. *See, e.g.*, USA FREEDOM Act, H.R. 3361, 113th Cong. (as passed by House, May 22, 2014) (explicitly revokes the authority for bulk collection).

21. *See, e.g.*, FISA Transparency and Modernization Act, H.R. 4291, 113th Cong. (as referred to Comm., Mar. 25, 2014) (revokes authority for bulk collection but creates new mechanism for expanded queries of telephone metadata). A similar approach is taken in a new Senate version of the USA FREEDOM Act introduced in the summer of 2014 by Sen. Leahy. *See* USA FREEDOM Act of 2014, S. 2685, 113th Cong (as voted against on a cloture motion to proceed on Nov. 11, 2014).

22. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 41 (D.D.C. 2013); Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).

predict, it seems the courts may be evolving toward a more nuanced approach than that taken in *United States v. Miller*[23] and *Smith v. Maryland*.[24] The ease with which metadata can now be aggregated and analyzed, along with the steady enhancement of the metadata itself, seems to be chipping away at the traditional precedent that transactional data in the hands of third parties does not have any Constitutional protection. If the data has some greater or lesser degree of Constitutional significance, then the examination of that data by the government is an especially sensitive operation. If that is the case, why would whatever Constitutionally protected interests exist be more secure if the operation were outsourced to private corporations? I think the answer lies in the belief that, because the Constitution principally protects individuals from government activity, keeping more data out of the hands of the government effects a de facto enhancement of personal liberty.

This belief, however, does not take into account the effect that the data retention mandate has on the very nature of the private entity. Telecommunications companies are in the business of moving data in forms such as voice, video, text, and internet traffic efficiently from one point to another. As discussed above, metadata generated by the communications process is held only if, and only for as long as, there is a business purpose in doing so.[25] Outside of limited internal business operations like fraud detection and cybersecurity, there typically is no need for companies to retain metadata for extended periods of time.[26] If the company is required to retain data for the use of intelligence agencies, it is no longer acting pursuant to a business purpose. Rather, it is serving the government's purpose; the company has become an agent or surrogate of the government in this context. The Constitutional benefit of having the data held by private entities is lost when, by the very act of compelling retention of that data for non-business purposes, the private entity becomes a functional surrogate of the government. Put another way, people initially may be comforted by the thought of their data remaining in the hands of telephone companies, but only to the extent that they believe the companies are truly independent of the government. When the companies are seen as

23. 425 U.S. 435, 443 (1976) (finding no Fourth Amendment protections for business records created through voluntary interactions with third parties).

24. 442 U.S. 735, 743–46 (1979) (applied *Miller* to find no Fourth Amendment protection for telephone call detail records).

25. Telephone providers typically note this principle in their user agreements or privacy policies. *See, e.g.*, *Verizon Privacy Policy Summary & AT&T Privacy Policy supra* note 18.

26. Telecom companies are allowed to access statutorily protected information for "rights and property" protection and for functions incidental to the delivery of the service. *See* 18 U.S.C. §§ 2072(b)(2), (5), 2511(2)(a)(i) (2012).

surrogates for or with the intelligence agencies, surely that comfort will dissipate.

The use of surrogates is not unfamiliar territory for the government. In fact, the government performs many of its functions through the vast infrastructure of federal contracting. Federal acquisition principles, which govern how federal agencies purchase goods or services from contractors, have always recognized that there are some functions so inherently governmental that they should never be outsourced.[27] Inherently governmental functions include activity "significantly affecting the life, liberty, or property of private persons"[28] and specifically include the "direction and control of intelligence and counter-intelligence operations."[29] Some aspects of the data retention concept may approach, if not exceed, this limit. While one might argue that the government still retains the "direction and control" of the collection operation, it is also true that the day-to-day decisions of how to retain the data, and what specifically to retain, will occur beyond the government's view, in very large and complex technical environments that are imperfectly understood outside the circle of those that actually operate them. The government may well have to rely on the companies' understanding and implementation of the retention requirements in the rapidly evolving and often proprietary environments that the companies control. This concern becomes more acute when the companies are also required to perform some form of analysis on the data before handing it to the government.

The current proposal is hardly the first time that the government has pushed the envelope on the "inherently governmental function" limit. The use of security contractors to perform quasi-military functions during the wars in Iraq and Afghanistan raised concerns about whether the government could maintain sufficient "direction and control" to ensure the proper behavior of its surrogates.[30] The investigations prompted by the often unsatisfactory and occasionally tragic results of that endeavor revealed the inherent difficulties in establishing effective oversight within a

---

27. *See* Memorandum from the Office of the Press Sec'y on Government Contracting to the Heads of Exec. Dep'ts and Agencies (March 4, 2009) *available at* http://www.whitehouse.gov/the_press_office/Memorandum-for-the-Heads-of-Executive-Departments-and-Agencies-Subject-Government/.

28. *See Circular No. A-76 Revised: Performance of Commercial Activities*, OFFICE OF MGMT. & BUDGET (May 29, 2003) at Attachment A, Section B(1)(a)(3), *available at* http://www.whitehouse.gov/omb/circulars_a076_a76_incl_tech_correction/.

29. *See* 48 C.F.R. § 7.503(c)(8) (2010).

30. *See, e.g.*, James Risen, *Before Shooting in Iraq, a Warning on Blackwater,* N.Y. TIMES, at A1, June 29, 2014, *available at* http://www.nytimes.com/2014/06/30/us/before-shooting-in-iraq-warning-on-blackwater.html?_r=0.

private entity.[31] It is noteworthy that the private security entities involved eagerly sought this role (as a surrogate) and were businesses constructed entirely for the purpose of providing these kinds of services to the government. By contrast, telecommunications providers are likely to resist any suggestion of data retention requirements, and operate businesses substantially unfocused on the collection of intelligence. The government's history with military contractors suggests that the benefits of outsourcing a difficult function can be lost

Effective oversight would be absolutely critical to any potential outsourcing of intelligence collection or analysis to private entities. One of the legacies of intelligence reform in the 1970s was a multi-layered oversight system designed to bring external review of intelligence agency activities while not compromising security. In the Executive Branch, oversight took the form of the President's Intelligence Oversight Board, which oversees the regulation of intelligence activities under Executive Order 12,333 and the various agency-specific implementations of that order.[32] Inspectors General within the Executive Branch are also involved in the oversight of intelligence activities, as is the PCLOB.[33] Intelligence agencies are subject to Congressional oversight, most directly through the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Congress has imposed myriad reporting requirements in the National Security Act, the FISA and many of the periodic Intelligence Authorization Acts.[34] Finally, the Courts exercise supervision of surveillance activities within the United States (and those targeting U.S. persons outside the United States) pursuant to FISA. As recently declassified opinions have confirmed, the FISC not only scrutinizes applications for surveillance authority but also is significantly involved in the "minimization" process applied to the collected information.[35]

---

31. *See* JENNIFER K. ELSEA, CONG. RESEARCH SERV., R40991, PRIVATE SECURITY CONTRACTORS IN IRAQ AND AFGHANISTAN: LEGAL ISSUES (2010) at 1-2 *available at* https://www.fas.org/sgp/crs/natsec/R40991.pdf.

32. *See* Exec. Order 12,333, 3 C.F.R. § 200 (1981), *reprinted as amended in* 50 U.S.C. § 401 app. at 16–30 (2012).

33. *See, e.g.*, 50 U.S.C. §§ 403q (CIA Inspector General), 3033(3)-(5)(A), (Inspector General of the Intelligence Community), 3602 (NSA Director of Compliance) (2012); *see also* 42 U.S.C. § 2000ee(c)-(d) (2006 & Supp. V 2012) (PCLOB enabling statute).

34. *See* 50 U.S.C. §§ 1808, 1826, 1846, 1862, 1871(a), 1881f (2012) (Congressional reporting requirements for various FISA operational authorities).

35. *See, e.g.*, Memorandum Opinion, In re Application of the Federal Government for an Order Requiring Production of Tangible Things from [Redacted], [Redacted], at 79–81 (FISA Ct., Oct. 3, 2011) [hereinafter Memorandum Opinion], *available at* http://www.lawfareblog.com/wp-content/uploads/2013/08/162016974-FISA-court-

Aside from the possible involvement of the FISC, none of these oversight mechanisms relate to private entities. All of the government facing oversight mechanisms derived from the Fourth Amendment restraints on government action[36] Oversight mechanisms in the private sector do not share that pedigree. Private companies conduct internal oversight to ensure that their employees comply with company policy; company policy, in turn, requires compliance with all relevant fiduciary, statutory, regulatory, and contractual requirements.[37] As in the case of data retention practices, corporate policy and oversight mechanisms are specifically tailored to the business. In telecommunications companies, customer privacy is the subject of oversight—but that oversight arises mostly from a contractual obligation. The common practice in the industry is to publish a privacy policy that explains what information the company collects, how it will use the information, and with whom it will share the information.[38] These policies may implement regulatory requirements, but also may exceed the protections required by regulation. Corporate oversight focuses on putting safeguards in place to implement the privacy policies, detecting violations of the privacy policy, assessing the need to issue notices or seek customer consent, and remediating improper disclosures of private data.

So, if data retention and analytical requirements make some telecom employees surrogates for government intelligence agencies, will existing oversight mechanisms be sufficient? I think that the answer is clearly no. Without substantial changes, the government facing mechanisms cannot be brought to bear on the telecom employees. Similarly, the in-house oversight structures do not contemplate governmental activity occurring within the private company. In order to establish the requisite direction and control, every company that is compelled to enter this new relationship with the intelligence agency will have to construct appropriate oversight mechanisms. To achieve uniform protection, these new mechanisms would have to be consistent in each company. Who would enforce such

---

opinion-with-exemptions.pdf; Primary Order, In re Application from the Federal Government for an Order Requiring that Production of Tangible Things from [Redacted], BR 08-13, at 17–20 (FISA Ct. Mar. 2, 2009) [hereinafter Primary Order], *available at* http://www.dni.gov/files/documents/section/pub_March%202%202009%20Order%20from%20FISC.pdf.

36. U.S. CONST. amend. IV.

37. *See, e.g., Verizon Code of Conduct*, VERIZON, *available at* http://www.verizon.com/about/sites/default/files/Verizon-Code-of-Conduct.pdf. Verizon's code details requirements for employees to comply with various legal obligations and describes internal enforcement of the same. For example, the Code requires the customer information. *See id. at sec. 4.1.1.*

38. *See Verizon Privacy Policy Summary*, *supra* note 18; *AT&T Privacy Policy*, *supra* note 18.

consistency and monitor the operation of these new structures? Most likely those tasks would fall to the same institutions that now oversee government activities (Congress, the courts, and Executive Branch agencies). In light of recent events, all of these institutions have been criticized for failing to question the development of the bulk collection program, and their critics portray them as sclerotic and self-referential. If any of this criticism is valid, then these institutions need substantial refurbishment before they can take on the creation of a new layer of oversight within private companies. But if such rejuvenation is possible, then wouldn't it be more efficient to bring enhanced oversight to bear in the government space, and leave the current collection paradigm intact?

The proposed outsourcing certainly does not offer any promise of efficiency. Under current conditions, the government would have to oversee the construction of collection and oversight mechanisms in several telecommunications companies just to maintain access to the stores of telephony metadata that appears to have been involved in the bulk collection program. Current conditions, however, are never persistent in technology. Already, telecommunications networks are evolving beyond traditional switched telephony. Voice over Internet Protocol ("VoIP") technologies handle voice traffic over the Internet (as opposed to the telephony networks) and already account for a substantial portion of voice traffic.[39] Even more dramatic has been the rise of "over the top" ("OTT") applications that use peer to peer or other technologies to establish direct connections between users over the Internet. In 2012, one such application (Skype) accounted for 34% of all international voice calling minutes (more than any other single provider).[40] VoIP and over the top applications may traverse IP networks operated by a large telecommunications company (most of which are also Tier 1 Internet Service Providers), but they do so as Internet traffic (not telephony) and thus the equivalent of call detail records reside with the VoIP or OTT provider, and not with the telecommunications company (which is simply the conduit for the IP traffic).[41] If the U.S. intelligence agencies were to commit to the outsourced

39. For a simplified technical explanation of VoIP, *see Understanding VoIP*, PACKETIZER, http://www.packetizer.com/ipmc/papers/understanding_voip/.

40. Phil Goldstein, *Report: Skype Makes Up One-Third of All International Phone Traffic*, FIERCE WIRELESS (Feb. 15, 2013), http://www.fiercewireless.com/story/report-skype-makes-one-third-all-international-phone-traffic/2013-02-15 (providing statistics for VoIP and Skype).

41. For example, a company like Verizon might carry a Skype call, but that call would simply be in the form of individual packets traversing Verizon's network. Only the provider (Skype) would re-assemble those packets on either end of the communication and thus know the identity of the user on either end of the call. *See* Goldstein, *supra* note 40.

solution to obtain telephony metadata, they would need to approach each successive VoIP or OTT application owner to establish access equivalent to the CDRs they obtain under the existing program. The technical difficulties multiply if the intelligence agencies were to eventually seek the same sort of access to IP metadata from Internet Service Providers.

Finally, the commercial effect on U.S. companies of outsourcing collection ought to be considered. No telecommunications company will be eager to undertake the increased responsibility, scrutiny, and liability entailed by having its employees become surrogates for the government in the collection of intelligence. More troubling for large U.S. telephone companies (all of which have extensive operations outside of the U.S.) is the effect in the international market of overt association with a U.S. intelligence agency.[42] There is a negative effect even when that relationship is compelled. The effect of an ongoing and official surrogacy relationship would doubtless be far more lasting and substantial. U.S. companies would become routinely subject to the same suspicions that, prior to the Snowden disclosure, some in the U.S. government had leveled at certain foreign corporations.[43]

CONCLUSION

All of the foregoing reasons, in my view, argue for maintaining the current structure under which intelligence agencies retain and analyze data that has been obtained from telecommunications companies in an "arm's length" transaction compelled by a FISA order. I think the proposal to outsource this work to surrogates in the private sector is a futile attempt to sidestep the difficult work that needs to be done to restore public confidence in intelligence agencies. I think that the best path forward is to focus on the repair and enhancement of existing oversight mechanisms, as well as on adjustments to the scope of FISA authorities. This last point alone will require a careful re-balancing of privacy and security interests—a process that took several years when it last occurred in the 1970s.[44] The

---

42. *See* Eamon Javers, *Is a Snowden Effect Stalking U.S. Telecom Sales?*, CNBC (Nov. 15, 2013, 12:16 PM), http://www.cnbc.com/id/101202361; *see also,* Anton Troianoski & Danny Yadron, *German Government Ends Verizon Contract*, WALL ST. J. (June 26, 2014 2:54 PM), http://online.wsj.com/articles/german-government-ends-verizon-contract-1403802226.

43. *See, e.g.*, MIKE RODGERS & DUTCH RUPPERSBERGER, HOUSE OF REPRESENTATIVE PERMANENT SELECT COMM. ON INTELLIGENCE, INVESTIGATIVE REPORT ON U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE (2012), *available at* https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20%28FINAL%29.pdf.

44. The reform period in Congress ran from the establishment of the Church Committee on January 27, 1975 through the passage of FISA in 1978. *See* KRIS &

adjustments to intelligence authorities made in the immediate aftermath of 9/11 should not persist or vanish[45] by default simply because we cannot bring ourselves to undertake deliberate reform.

WILSON, *supra* note 1 at Chapter 2, sec. 2.3, Chapter 3, sec. 3.7. In the Executive Branch, active reform continued until the issuance of Executive Order 12,333 in 1981. *See id.* At Chapter 2, sec. 2.7.

45. Under current law, Section 215 of the USA PATRIOT Act sunsets on June 1, 2015. *See* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 102(b), 120 Stat. 192 (2006).