Systematic government access to private-sector data in the United States

Stephanie K. Pell*

Abstract

- After the September 11 (9/11) attacks, law enforcement's mission expanded to include, at times even prioritize, the general 'prevention, deterrence and disruption' of terrorist attacks, which presumed a new emphasis upon threat detection and identification by analysing patterns in larger, less specific bodies of information.
- Moreover, after 9/11, law enforcement was integrated into a much larger intelligence gathering operation directed at 'connecting the dots' proactively, in order to avert the *next* terrorist attack. This new focus, spread across a broad range of federal and state agencies, has created a voracious appetite for information—data found most often in the possession of industry, given consumer use of new technologies to facilitate personal, social, business, and economic transactions.
- Indeed, the unprecedented level of 'third-party' possession of information inevitably makes the private sector the most reliable and comprehensive source of information available to law enforcement and intelligence agencies alike. Notwithstanding the impacts on business costs or innovation—whether for a criminal or intelligence terrorism matter or more traditional crimes where perpetrators leave electronic fingerprints with a host of third parties—there is an expectation by law enforcement, intelligence agencies, and even legislators that industry third parties will facilitate real time government access to data when needed, and that these data will be in possession of the relevant private entities if and when a government agency realizes their potential investigative value.

Introduction and overview

Following the September 11 (9/11) attacks, the mission of police and prosecutors expanded dramatically. Before that date, most law enforcement resources were allocated for the post-facto investigation or prospective prevention of specific crimes (like organized crime and drug trafficking investigations), with far fewer devoted to intelligence collection and threat detection to prevent an attack upon the homeland. After 9/11, however, law enforcement's mission expanded to include, at times even prioritize, the general 'prevention, deterrence and disruption' of terrorist attacks, which presumed a new emphasis upon threat detection and identification though analysis of patterns in larger, less specific bodies of information. Moreover, after 9/11, law enforcement was integrated into a much larger intelligence gathering operation directed at 'connecting the dots' proactively, in order to avert the *next* terrorist attack. This new focus, spread across a broad range of federal and state agencies, has created a voracious appetite for information—data found most often in the possession of industry, given consumer use of new technologies to facilitate personal, social, business, and economic transactions. Indeed, the unprecedented amount of 'third-party' possession of information inevitably makes the private sector the most reliable and comprehensive source of information available to law enforcement and intelligence agencies alike. Notwithstanding the impacts on business costs or innovation—whether for a criminal or intelligence terrorism matter or more traditional crimes where perpetrators leave electronic fingerprints with a host of third parties—law enforcement, intelligence agencies and even legislators expect that industry third parties will facilitate real time government access to data when needed, and that these data will be in possession of the relevant private

* Principal, SKP Strategies, LLC; former Counsel to the House Judiciary Committee; former Senior Counsel to the Deputy Attorney General, US Department of Justice; former Counsel to the Assistant Attorney General, National Security Division, US Department of Justice; and Former Assistant US Attorney, Southern District of Florida. The author would like to thank Fred Cate, Jim Dempsey, Jim Green, Ron Lee and Christopher Soghoian for their feedback and assistance.

- This paper will explore the potential applications of systematic government access to data held by third-party private-sector intermediaries that would not be considered public information sources but, rather, data generated based on the role these intermediaries play in facilitating economic and business transactions (including personal business, such as buying groceries or staying at a hotel on vacation).

entities if and when a government agency realizes their potential investigative value.

Perhaps the most visible post-9/11 expression of the government's appetite for information came in the form of a data mining project led by the Defense Advanced Research Projects Agency (DARPA), originally named 'Total Information Awareness' (TIA), but later, significantly, renamed 'Terrorism Information Awareness'.[1] The revised name might have suggested a new and limiting precision in the scope of the project, but this change should not be read to signal any change, either in practice or in the programme's ultimate goal. In 2002, John Poindexter, a retired Admiral and director of DARPA's Information Awareness Office, identified the 'transaction space' as one of the 'significant new data sources that need to be mined to discover and track terrorists'.[2] This 'transaction space' included data encompassing communications, financial, education, travel, medical, veterinary, country entry, place/event entry, transportation, housing critical resources, and government records.[3] As part of the TIA programme, DARPA 'red teams' would develop model attack scenarios, then determine the types of transactions that would be necessary to carry out such attacks in reality.[4] These transactions could form patterns that would be discernable in databases to which the government would have lawful access.[5] Having developed targetable patterns of attack precursor behavior, the government could then search across databases to detect the presence of those patterns.[6]

While the funding for this kind of 'total information awareness' programme was ultimately terminated by Congress in 2003, following protests about the programme's privacy impact, today,[7] in a time when even more social and business transactions are facilitated by technology, we once again perceive signs of the government's quest for a kind of comprehensive information awareness and access. The FBI, for example, recently put out a formal 'Request for Information'(RFI) that appears to reflect its plans to build a comprehensive social media monitoring system.[8] Moreover, on 16 February 2012, the House Homeland Security Committee held a hearing entitled 'DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Protecting Privacy'.[9]

Although government monitoring of social media and other public information sources raises legitimate privacy concerns, this paper will explore the potential applications of systematic government access to data held by third-party private-sector intermediaries that would not be considered public information sources but, rather, data generated based on the role these intermediaries play in facilitating economic and business transactions (including personal business, such as buying groceries or staying at a hotel on vacation). For the most part, US laws and regulations do not directly authorize, much less formally require, unmediated government access to data held by third-party intermediaries. While US law mandates some ongoing third-party disclosures of various types of information involving, for example, cargo and passengers coming into the US from abroad or financial data that might assist the government in identifying money laundering or terrorist financing, these data are divulged pursuant to regulatory requirements, which presumably assist in preventing unmediated government access to third-party data. For the purposes of this paper then, the term 'systematic' is used to denote any or all of the following that could arguably permit the government either to obtain information without any process or to use process to obtain such a broad or voluminous amount of information that an unnecessary and perhaps ongoing

1 Fred H. Cate, 'Government Data Mining: The Need for a Legal Framework', (2008) 43 Harv. C.R.-C.L. L. Rev. 435, 449.

2 John Poindexter, Director, Info. Awareness Office, Overview of the Info. Awareness Office, Prepared Remarks for Delivery at DARPATech 2002 Conference (2 Aug. 2002), at 2, available at: <http://www.fas.org/irp/agency/dod/poindexter.html>.

3 See Cate (n 1) at 450 (describing a slide consisting of categories of transaction data shown by Admiral Poindexter at the DARPA Tech2002 Conference).

4 Info. Awareness Office, U.S. Dep't of Def., Report to Congress Regarding the Terrorism Information Awareness Program 14 (2003), available at: <http://epic.org/privacy/profiling/tia/may03_report.pdf>.

5 Id.

6 Id.

7 See Cate (n 1), at 450–51.

8 See Jaikumar Vijayan, 'FBI Seeks Social Media Monitoring Tool', (2012) 14 Feb. ComputerWorld, available at: <http://www.computerworld.com/s/article/9224235/FBI_seeks_social_media_monitoring_tool>.

9 See <http://homeland.house.gov/hearing/subcommittee-hearing-dhs-monitoring-social-networking-and-media-enhancing-intelligence>.

over-collection of information could readily occur: (1) exploiting[10] gaps in existing statutes regulating government access to certain types of data held by specific types of third parties; (2) government use of Executive Orders; (3) government operating practices (which may include informal partnerships with private entities); or (4) exploiting the lack of constitutional protections against and statutory prohibition of government access to certain types of data held by third parties. The ways in which systematic government access may operate are rarely transparent, often presenting themselves only when a controversy surfaces in the press, as in the case of the Terrorist Surveillance Program (a programme of the National Securtiy Agency (NSA) where, without any court order, the NSA, assisted by major telecommunications companies, intercepted communications when at least one party was located in the United States).[11]

Perhaps one good threat assessment deserves another. Just as DARPA's TIA programme required analysts to design terrorist attack scenarios, then reverse engineer the transactions necessary to complete the attack, the same type of critical eye is needed to discern if the government, even for legitimate purposes and consistent with authorized mandates, can obtain systematic access to third-party data, whether by voluntary disclosure or through compelled legal process.

US national legal context and fundamental principles

The primary constitutional limit on the government's ability to obtain private or personal information is the Fourth Amendment, which prohibits unreasonable searches and seizures. Supreme Court Fourth Amendment case law has prescribed certain tests to determine whether a search has occurred, which is the preliminary question to be answered before turning to whether any particular search is unreasonable. Justice Harlan's famous concurrence in *Katz v United States*,[12] now commonly referred to as the *Katz* test, guides courts in determining what constitutes a search under the Fourth Amendment. This test has both subjective and objective elements. Courts must determine: (1) whether the government conduct in question violates an individual's subjective expectation of privacy; and (2) whether that expectation of privacy is one that society recognizes as reasonable. More recently, in *United States v Jones*,[13] a case involving the government's warrantless attachment and use of a GPS device to track the movement's of Jones' car for 28 days, Justice Scalia wrote a majority opinion articulating a new doctrine for determining what constitutes a Fourth Amendment search. This new trespass-based test is satisfied when: (1) a 'trespass' occurs; (2) the trespass is to a target enumerated in the Fourth Amendment ('persons, houses, papers, or effects'); and (3) it occurs with the intent 'to find something or to obtain information'.[14]

The Fourth Amendment, however, provides little to no protection for data stored by third parties. In *United States v Miller*,[15] the Supreme Court held that there is no reasonable expectation of privacy in information held by a third party. The case concerned cancelled checks and the Court reasoned that the respondent 'can assert neither ownership or possession' in documents 'voluntarily conveyed to banks and exposed to their employees in the ordinary course of business'.[16] Accordingly, the Fourth Amendment was not implicated when the government sought access to the records. Later, in *Smith v Maryland*,[17] the Court reinforced what is now called the 'third party doctrine', holding that the Fourth Amendment does not apply to transactional information associated with making phone calls (eg time/date/length of call and numbers dialled) because that information is knowingly conveyed to third parties to connect the call and phone companies record the information for a variety of legitimate business purposes. These cases established the longstanding precedent that the Fourth Amendment is essentially inapplicable to records in the possession of third parties.

The privacy protections that do exist for third party records are primarily found in statutes enacted by Congress specifically in response to Supreme Court opinions limiting Fourth Amendment protections. Additional privacy protections may be found in agency guidelines and privacy policies, some of which exist because Congress has mandated their creation by statute. While it is beyond the scope of this paper to conduct an analysis of the full scope of such policies (some of which may be classified) and their impact on

10 The term 'exploiting' as used in this paragraph is not meant to convey a sinister motive. Rather, if the government is not prohibited from collecting data by the Constitution or by statute, then it can lawfully collect that data consistent with internal agency guidelines and authorized investigative activities, with very limited, if any, barriers.

11 See 'Real time' communications content at pp. 4–5.

12 *Katz v United States*, 389 U.S. 347, 361 (1967).

13 132 S.Ct. 945 (2012).

14 See Orin Kerr, 'The New Doctrine of What is A Fourth Amendment Search', Volokh Conspiracy Blog, 23 Jan. 2012, available at: <http://volokh.com/2012/01/23/the-new-doctrine-of-what-is-a-fourth-amendment-search/>.

15 425 U.S. 435 (1976).

16 Id. at 442–43.

17 442 U.S. 735 (1979).

the government's systematic access to third-party records, policy that is managed by political leadership of an agency is always subject to change, for better or worse.

Statutory overview and analysis

For the purposes of exploring potential systematic government access to third-party private-sector data, it is often useful to think about statutory privacy protections in terms of (a) what kind of third-party private-sector entities they regulate and (b) what type of information they regulate. Sometimes a statute will regulate the disclosure of a specific type of information to the government, but only by a specific type of third party. Thus, the disclosure of the same type of information by a third party not covered by the statute could lawfully occur without any legal process. In the service of exploring the potential for systematic government access, this section will analyse the primary statutes regulating third-party disclosure of information to the government, the Electronic Communications Privacy Act (ECPA),[18] the Foreign Intelligence Surveillance Act (FISA),[19] National Security Letters (NSLs),[20] and the Right to Financial Privacy Act (RFPA).[21] These statutes, while certainly not the only authorities affecting government access to and retention of third-party private-sector data, provide the richest opportunity for discussion of systematic government access to these data. These key statutes govern various aspects of government access to: (1) electronic communications; (2) financial data; and (3) other records in the possession of third parties for both criminal and national security investigations. The discussion below will group these authorities as they relate to these three major categories of information.

Electronic communications data: ECPA, FISA, and NSLs

'Real time' communications content

The Wiretap Act (Title I of ECPA) governs law enforcement access to 'real time' wire, oral and electronic communications in criminal investigations. For the federal government to gain access to these real time communications, it must establish, in a written application to a judge of competent jurisdiction, that there is probable cause to believe that (1) an individual is committing, has committed, or is about to commit a particular offence enumerated in the Wiretap Act and (2) particular communications concerning that offence will be obtained through the requested interception.[22] In addition to this showing of probable cause, the government must also demonstrate that other normal investigative procedures have been tried and have failed, or reasonably appear unlikely to succeed if tried or would be too dangerous to execute.[23] The Wiretap Act also limits this intrusive surveillance tool to specific crimes listed in the statute. This list is extensive and includes a broad range of terrorism-related statutes. In the case of terrorism and national security investigations, however, the federal government's ability to intercept real time communications is often not limited to authorities provided in the Wiretap Act. Such investigations—involving collection of foreign intelligence about 'foreign powers' or 'agents of foreign powers' who may or may not be engaged in criminal activities—are often more readily and appropriately pursued under FISA authorities. Accordingly, FISA authorizes the interception of real time wire, oral, and electronic communications when, by written application to the FISA Court, the government demonstrates that there is probable cause to believe that: (1) the target of the electronic surveillance is a foreign power or agent of a foreign power; and (2) each of the facilities or places at which electronic surveillance is directed is being used, or is about to be used by a foreign power or an agent of a foreign power, which includes a so-called 'lone wolf' (ie an unaffiliated foreign individual posing a threat).[24]

Warrants granted pursuant to the Wiretap Act are often called 'super warrants' and considered by many privacy advocates to be the 'gold standard' for limiting unconstitutional collection or over-collection of communications content. This characterization derives from several elements, including but not limited to: (1) a probable cause showing predicated upon the discovery of evidence of a specific crime; (2) the minimization of non-relevant communications; and (3) a special review process at the DOJ in Washington DC (Main Justice) governing all wiretap applications.[25] While a comprehensive comparison of the Wiretap Act and

18 18 U.S.C. §§ 2511–2520; 18 U.S.C. §§ 2701–2712; 18 U.S.C. §§ 3121–3127.

19 50 U.S.C. §§ 1801–1862.

20 There are five provisions of law that authorize the FBI to issue five types of NSLs: 12 U.S.C. § 3414(a)(5)(A); 18 U.S.C. § 2709; 15 U.S.C. § 1681u; 15 U.S.C. § 1681v; 50 U.S.C. § 436.

21 12 U.S.C. §§ 3401–3422.

22 18 U.S.C. §§ 2518(3)(a),(b).

23 18 U.S.C. § 2518(c).

24 50 U.S.C. § 1805.

25 See 18 U.S.C. §§ 2516(1), 2518(3)(a),(b), 2518(5).

FISA is beyond the scope of this paper, FISA also contains minimization and oversight provisions, including its own specialized review process at Main Justice and a certification by a high level official that such information cannot be obtained by normal investigative techniques.[26] FISA's probable cause standard, however, is premised on the collection of foreign intelligence relative to foreign powers or agents of foreign powers, rather than to collection of evidence a crime, arguably permitting a broader, more flexible exercise of government surveillance powers.

The extent to which the differences between FISA and the 'gold standard' Wiretap Act (many of which are not mentioned here) may facilitate systematic government access to real time communications content travelling on third-party networks is unclear, largely because a great deal about how the government interprets and uses its FISA authorities is classified. One infamous example of systematic government access, however, surfaced when the *New York Times* reported that major telecommunications companies granted the NSA *warrantless* access to monitor international telephone calls and electronic communications (like email), even when one party was a US person located on US soil.[27] This so called 'Terrorist Surveillance Program' (TSP), which circumvented FISA, was authorized by President Bush via a classified Executive Order and facilitated the NSA's warrantless spying on millions of Americans' telephone calls and email exchanges.[28] This systematic government access evidently developed through a public–private partnership in which NSA informally arranged with top officials from telecommunications companies to gain access to switches carrying America's communications without warrants or court orders.[29] After the TSP programme was exposed, industry members sought retroactive immunity to avoid adverse consequences stemming from this informal cooperation.[30]

Stored communications content

Title II of ECPA, the Stored Communications Act (SCA),[31] governs law enforcement access to content communications when in the possession of a third party providing an 'electronic communications service' (ECS)[32] or a 'remote computing service' (RCS)[33] to the public. These definitions are the product of how the Internet and Internet-based services existed in 1986, the year the SCA was enacted by Congress. While the definition of RCS certainly reflects Congress' understanding that there could and would be third-party storage of content ('computer storage or processing services'), Congress could not have foreseen the extent to which various types of third-party storage, used by consumers and businesses alike, would become a booming business model due to an explosion in cloud-based services. In 1986, third-party storage was prohibitively expensive, causing most people and businesses using computers to store electronic content locally on a hard drive or floppy disk.

Consistent with Fourth Amendment doctrine, law enforcement normally must get a warrant in order to search and seize a laptop, desktop, or thumb drive. In 1986, Congress extended the warrant protection via statute to communications content stored in an ECS (such as unopened email),[34] but did not extend full warrant protections to communications content in RCS storage.[35] Today, a large amount of data stored in the cloud (including opened email) is arguably in RCS storage. Accordingly, the government can compel third-party providers to disclose communications content in RCS storage with an 18 USC § 2703(d) Order (a court order under which the government must show, with 'specific and articulable facts,' that there are reasonable grounds to believe that the information sought is 'relevant and material' to an ongoing criminal investigation) or even with a subpoena.[36] This disparity in the level of privacy protections given to information stored 'in the cloud' versus content stored on a laptop, combined with the sheer amount of content now in third-party storage, has given the government much greater access to private-sector communications content. Indeed, a major cloud provider testified at a congressional hearing that the weak ECPA privacy protections afforded information stored 'in the cloud' limits the expansion of the cloud market, particularly to foreign

26 See 50 U.S.C. §§ 1804(a)(5), 1804(a)(7)(C).

27 See Jon D. Michaels, 'All the President's Spies: Private–Public Intelligence Partnerships in the War on Terror', (2008) 96 Cal. L. Rev. 901, 910.

28 Id.

29 Id.

30 See *Hepting v ATT Corp.*, 671 F.3d 881 9th Cir. 2011, (upholding the constitutionality of a 2008 law that gave telecom companies a path to retroactive immunity from charges of misconduct, including privacy violations, for cooperating with the Bush administration's warrantless wiretapping efforts).

31 18 U.S.C. §§ 2701–2712.

32 An electronic communication service (ECS) is 'any service which provides to users thereof the ability to send or receive wire or electronic communications.' Examples include telephone or email services. 18 U.S.C. § 2510(15).

33 A 'remote computing service' ('RCS') is a 'provision to the public of computer storage or processing services by means of an electronic communications system.'" 18 U.S.C. § 2711(2). Generally speaking, an RCS is provided by an off-site computer that stores or processes data for a user such as cloud-based online backup services.

34 See 18 U.S.C. § 2703(a).

35 See 18 U.S.C. § 2703(b).

36 18 U.S.C. §§ 2703(b), (d).

customers who are concerned that the US government has overly broad access to cloud-stored information.[37] In the 2010 *Warshak* opinion, however, the Sixth Circuit held that 'if government agents compel an ISP to surrender the contents of a subscriber's emails, those agents have thereby conducted a Fourth Amendment search, which necessitates compliance with the warrant requirement absent some exception'.[38] Moreover, the Court held that 'to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.'[39] While not a Supreme Court opinion or an amendment to ECPA, *Warshak* is a strong step towards the protection of content 'in the cloud'.

Stored non-content communications data

Arguably the greatest potential for unmediated government access to *non-content* communications data is due in part to gaps in existing statutes and government practices. The SCA governs law enforcement access to stored non-content communications data when it is in possession of a third party providing an ECS or RCS service to the public. The SCA, however, only regulates non-content data (eg transactional or other records pertaining to subscriber and customer names, addresses, length and type of service, temporarily assigned network address, means and source of payment) with respect to entities providing ECS and RCS services. If this non-content data is in the possession of a third party that is not acting as a public ECS or RCS, then the SCA does not provide any level of protection for the data. Without any statutory protection, third parties can, if they choose, voluntarily disclose data without any process. For example, when security researchers discovered that Apple and Google phones were collecting and transmitting back to the companies information about a device's nearby WiFi access points and geo-location data,[40] the transmission of the location data was arguably not a function of an ECS or RCS service and thus would not receive the SCA protections otherwise afforded to historical location data. The government could, therefore, compel the disclosure of that location data with a subpoena (when the SCA would otherwise require a court order) or it could be disclosed to the government voluntarily by a third-party entity, in the absence of any emergency and without any process.

Moreover, the SCA does not prohibit the entities that provide public ECS and RCS services from disclosing non-content data to other non-governmental entities. Once in the possession of these fourth-party entities (like data brokers), which are not providing public ECS and RCS services, the data can be sold or otherwise disclosed to the government without process. These fourth-party commercial data brokers collect information from a range of third parties (not just those regulated by the SCA) and can provide 'one stop shopping' for law enforcement and intelligence agencies alike.[41]

The SCA also contains one of the five National Security Letter (NSL)[42] authorities, a series of foreign intelligence statutory authorities allowing the government to compel certain types of non-content data, principally from communications providers, financial institutions (defined very broadly), and credit agencies. Similar to subpoenas, the FBI and other designated intelligence agencies can issue NSLs without court authorization or, unlike subpoenas, without even review by a prosecutor. The NSL authority found in the SCA permits the government to obtain subscriber, customer and, the government argues, other types of transactional records[43] in the possession of ECS and RCS providers (eg non-content data pertaining to telephone and email communications).

Three different DOJ Inspector General (IG) Reports released between 2007 and 2010 document a series of abuses concerning the FBI's use of NSL authorities. While these reports identify several types of abuses, two key problems are particularly relevant to the examination of when and how the government can get unmediated access to third-party data. First, the FBI, in violation of ECPA and various internal guidelines, used 'exigent letters' (*ad hoc* instruments with implied legal authority where none existed) to acquire information from communication providers with the promise that

37 See ECPA Reform and the Revolution in Cloud Based Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties for the H. Comm. On the Judiciary, 111th Cong. (2010) (testimony of David Schelhause, Executive Vice President and General Counsel, Salesforce.com at 40) (explaining that customers considering storing their information 'in the cloud' want assurances that the U.S. government will not access their data without appropriate due process), available at: <http://judiciary.house.gov/hearings/hear_100923.html>.

38 *United States v. Warshak*, 631 F.3d 266, 286 (2010).

39 Id at 288.

40 See Julia Angwin &and Jennifer Valentino-Devries, 'Apple, Google Collect User Data', The Wall Street Journal, 21 April 21, 2011 available at: <http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html>.

41 See Michaels (n 27), at 918.

42 18 U.S.C. § 2709.

43 See 18 U.S.C. § 2709. The Washington Post reported that the government was seeking from Congress what it characterized as a 'technical clarification' to § 2709 to facilitate the collection of transactional records. Others characterized the government's request as an expansion of collection authority under § 2709. See Ellen Nakashima, 'White House Proposal Would Ease FBI Access to Records of Internet Activity', 29 July 29, 2010, available at: <http://www.washingtonpost.com/wp-dyn/content/article/2010/07/28/AR2010072806141_pf.html>.

actual process (like subpoenas) would follow.[44] Going forward, this kind of subterfuge with promises that 'process is on its way' should raise red flags for all public–private relationships. Second, from April 2003 through January 2008, employees of certain communications providers were located in the FBI's Communications Assistance Unit (CAU), which included being provided with FBI email accounts and access to the CAU computer share drive.[45] These on-site providers' employees regularly attended CAU unit meetings and were treated by CAU personnel as 'team members'.[46] While the IG recognized that the collegial relationship between the co-located personnel fostered a productive working relationship, the 2010 report also notes that the 'proximity of the on-site providers' employees to the CAU personnel, combined with the lack of guidance supervision, and oversight of their interactions with FBI employees . . . contributed to some of the most serious abuses identified in this review'.[47] Indeed, in this instance, there appeared to be a merger of the 'public' and 'private' roles.[48]

Although the IG's unclassified reports provided a great deal of insight into specific NSL abuses, much of how the government interprets and uses its foreign intelligence authorities, including FISA authorities, to acquire non-content communications data for foreign intelligence investigations remains unknown to the public. In addition to its use of NSLs to compel various types of non-content data, the government can, in foreign intelligence and international terrorism investigations, seek a FISA Court Order, pursuant to Sec. 501 of FISA, to require third-party production of any 'tangible thing', which can include business records, as the title of Sec. 501 indicates.[49] While the DOJ made some general information available about its uses of Sec. 501 Orders during the 2009 Congressional USA PATRIOT Act reauthorization hearings (eg to obtain transactional information that did not fall within the scope of other national security authorities like NSLs),[50] presumably the scale and specific types of information collected pursuant to Sec. 501 is classified and thus unknown.

While perhaps a necessary function of the protection of classified sources and methods, the lack of public information about how the government interprets and uses its foreign intelligence authorities makes it difficult to determine when and how systematic government access to non-content data may occur. Consider, for example, a May 2006 story in *USA Today* involving another government–telecommunications partnership where companies transferred large amounts of non-content data pertaining to telephone and Internet communications to the NSA, some even derived from purely domestic exchanges.[51] *USA Today* also reported that Qwest, a company which 'was uneasy about the legal implications of handing over customer information to the government without warrants', refused to cooperate in the broad disclosures.[52] In response to this resistance, a Qwest executive has alleged that the NSA retaliated by cancelling lucrative contracts.[53]

'Real time' non-content communications data

While the SCA regulates government access to stored non-content data in the possession of certain types of third-party providers, Title III of ECPA (the pen register and trap and trace device statute, commonly referred to as 'Pen/Trap') governs law enforcement's ability to acquire 'real time' transactional information about phone calls.[54] While the DOJ's public manual on *Searching and Seizing Computers* does not give a detailed list of all of the specific types of transactional information that can be obtained with a Pen/Trap order, it notes that the statute's '"dialing, routing addressing [and/or] signaling information" encompasses almost all non-content information in a communication'.[55] The Electronic Frontier Foundation

44 See 'A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records', Oversight Review Division, Office of the Inspector General, January 2010, available at: <http://www.justice.gov/oig/reports/FBI/index.htm>.

45 Id. at 24.

46 Id. at 24–25.

47 Id. at 25.

48 Another example of a public–private interface involved Sprint Nextel developing a web interface to give law enforcement direct access to its subscribers' location data in order to cope with voluminous compelled disclosures of the data. *United States v. Pineda-Moreno*, 617 F.3d 1120, 1126 (9th Cir. 2010) (Kozinski, J. dissenting from denial of rehearing en banc).

49 50 U.S.C. § 1861.

50 See H.R. Rep. No. 111–382 at 15 (2009). These orders are often called Sec. 215 Orders to reflect the changes made to Sec. 501 by Sec. 215 of the USA PATRIOT Act, Pub. L. 107–56, Sec. 215 (26 Oct. 26, 2001).

51 Michaels (n 27), at 912, *citing* Leslie Cauley, 'NSA has Massive Database of Americans' Phone Calls', USA Today, 11 May 11, 2006, available at: <http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm>.

52 Id.

53 Michaels (n 27), at 913, *citing* Ellen Nakashima & and Dan Eggen, 'Former CEO Says U.S. Punished Phone Firm', Washington Post, 13 Oct.13, 2007, available at: <http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202485.html>.

54 See 18 U.S.C. §§ 3121–3126. In foreign intelligence investigations, the government may also use FISA Pen/Trap authorities. See 50 U.S.C. § 1842.

55 U.S. Department of Justice, Computer Crime and Intellectual Prop. Section, Criminal Div., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* at 154 (3rd edn., US Department of Justice 2009), at 154 [hereinafter *DOJ Manual*].

(EFF) has interpreted the scope of the DOJ's potential collection ability to include: the numbers a phone calls and receives; the starting and ending time of each call; the duration of each call; whether each call was connected or went to voicemail; and (although a disputed, controversial use of Pen/Trap) 'post-cut-through dialed digits' (digits dialled after a call is connected, like a banking PIN number or a prescription refill number).[56]

Enacted seven years after *Smith v Maryland*, the Pen/Trap statute was a congressional response to the Supreme Court's holding that the Fourth Amendment does not apply to transactional information associated with making phone calls. The USA PATRIOT Act then expanded the government's ability to use Pen/Trap to acquire 'real time' transactional information about email,[57] which the DOJ asserts, once again, could encompass almost all non-content information in a communication[58] and EFF explains may include: addresses of sent and received email; the time each email is sent or received; the size of each email that is sent or received; IP (Internet Protocol) addresses to include IP addresses[59] of other computers a target computer exchanges information with, as well as the communications ports and protocols used (which, in turn, can be used to determine the types of communications sent and the types of applications used).[60]

Concerns about how the Pen/Trap statute might facilitate unmediated government access to third-party data primarily derive from: (1) the statute's low certification standard; (2) certain types of information that might be collected; and (3) the scope and volume of information that can presumably be collected with a Pen/Trap order. Specifically, to obtain a Pen/Trap order, the government must only certify to a court that the information likely to be obtained is 'relevant to an ongoing criminal investigation'.[61] Since this certification does not require a court to *evaluate* any facts to determine if the information is likely to be relevant to an ongoing criminal investigation, there is no meaningful judicial oversight. Some have also raised concerns that law enforcement may use Pen/Trap to collect the URLs (website addresses) of websites visited, which could allow the tracking of what someone is reading while surfing the web.[62] Moreover, there is no limitation on the scope of information collected in a particular investigation, whether with single or multiple Pen/Trap orders. While certain types of investigations require a broad collection of phone and email transactional information, if there is no meaningful judicial oversight regarding the scope of such collection, the potential for unmediated government access to third-party data looms large.

Financial data: Right to Financial Privacy Act, NSLs

Just as the SCA and the Pen/Trap provisions of ECPA were a congressional response to the lack of Fourth Amendment protections afforded to electronic communications in the possession of third parties, Congress enacted The Right to Financial Privacy Act[63] in 1978, two years after the *Miller* decision, where the Supreme Court held that there was no reasonable expectation of privacy in documents voluntarily conveyed to banks and exposed to their employees in the ordinary course of business. The statute prohibits federal agencies from acquiring customer records from a financial institution without either the customer's consent or appropriate process, such as a search warrant or a judicial or administrative subpoena.[64] The statute, however, is subject to several exceptions, including disclosures required under other federal statues or rules, or for various administrative purposes.[65] Moreover, the Act does not control federal government acquisition of financial information from third parties that are *not* financial institutions, nor does it prohibit disclosures to state or local governments or private entities.[66] The Act also contains one of the five NSL authorities,[67] permitting the government to compel financial institution customer records in foreign intelligence investigations (eg 'open and closed checking and savings accounts, transactions records from banks, private bankers, credit

56 See: <https://ssd.eff.org/wire/govt/pen-registers>. With respect to 'post-cut-through dialed digits' or other communications content, the *DOJ Manual*, citing 18 U.S.C. § 3121(c), instructs that the 'government must also use "technology reasonably available to it" to avoid recording or decoding the contents of any wire or electronic communications. . . . Where there is no way to avoid the inadvertent collection of content though the use of reasonably available technology, DOJ policy requires that the government may not use any inadvertently collected content in its investigation.' See *DOJ Manual*, *supra* (n 55), at 155–56.

57 See Pub. L. 107–56, Sec. 216 (26 Oct. 26, 2001).

58 See *DOJ Manual supra* (n 55) at 155–56.

59 See *In re Application of United States*, 416 F. Supp. 2d 13, 18 (D.D,C, 2006) (approving Internet Pen/Trap order seeking specified non-content information, such as originating IP addresses).

60 See <https://ssd.eff.org/wire/govt/pen-registers>.

61 18 U.S.C. § 3122(b)(2).

62 See <https://ssd.eff.org/wire/govt/pen-registers>.

63 12 U.S.C. §§ 3401–3422.

64 12 U.S.C. § 3402.

65 12 U.S.C. § 3413(d).

66 12 U.S.C. §§ 3401 (1)-(3).

67 12 U.S.C. § 3414.

unions, thrift institutions, credit card companies, insurance companies, etc.').[68]

Following the 9/11 attacks, it was reported that the government gained unprecedented access to the world's banking databases through a relationship with the Society for Worldwide Interbank Financial Telecommunications (SWIFT), a Belgium-based cooperative that serves as 'the central nervous system of international banking'.[69] At that time, SWIFT purportedly carried information 'for nearly 8,000 financial institutions', which conducted 'up to 12.7 million financial transactions a day'.[70] While SWIFT executives 'insist[ed] that their organization's participation had not been voluntary' but, rather, was in compliance with US government NSLs, SWIFT's willing cooperation appeared to represent 'a significant departure from typical practice'.[71] The SWIFT example illustrates how the government may use statutory authorities to acquire vast amounts of information—in this case purportedly with mere NSLs—such that the information collection might be characterized as systematic government access *aided by* the cooperation of a 'friendly' third party (likely due to circumstances surrounding the 9/11 attacks).

Additional mystery regarding government access to financial data surrounds a government practice referred to as 'hotwatch' orders, 'issued pursuant to the All Writs Act. Such orders direct a credit card issuer to disclose to law enforcement each subsequent credit card transaction effected by a subject of [an] investigation immediately after the issuer records that transaction'.[72] A DOJ presentation obtained through a Freedom of Information Act (FOIA) request suggests that law enforcement's preferred way of obtaining a 'hotwatch' order is to contact a credit card company's security department and provide that department with an administrative subpoena and a court order for 'non-disclosure'.[73] While the scope of information obtained from 'hotwatch' orders is unclear, it is important to note that the data are provided in 'real time' and presumably will include information about the subject of the transaction (ie the type of purchase made or service conducted) which, in turn, can also reveal the location of the user at the time she made the transaction (in the case of a 'brick and mortar' business or institution). Indeed, the DOJ presentation characterizes credit card 'hotwatch' orders as 'real time tracking'.[74]

With respect to data stored by third parties outside of the United States, it is also worth noting that the US government can obtain bank or business records located abroad by serving subpoenas on branches of the bank or business located in the United States, even when disclosure would violate the foreign country's laws. Courts have upheld the use of these so-called 'Bank of Nova Scotia subpoenas' (named after the seminal case).[75] The *Bank of Nova Scotia* facts and reasoning have, however, been distinguished by other courts[76] and the cross-border issues associated with data held 'in the cloud' may ultimately provide more wrinkles to the *Bank of Nova Scotia* line of cases.

Other records in the possession of third parties

As previously noted, data not protected by the Constitution or regulated by statute such that a court order is required for its production can be compelled by the government with 'low level' process (ie subpoena or NSL) or even provided voluntarily to the government without any legal process. This 'lack of regulation' can potentially facilitate the kind of reported public–private partnerships with Western Union, Federal Express, and major airlines seen in the aftermath of the 9/11 attacks. Shortly after the attacks, then CIA director George Tenet invited Western Union executives to his

68 See Michaels (n 27), at 921, n 86 (listing various types of customer records that may be obtained from different types of financial institutions pursuant to 12 U.S.C. § 3414).

69 Michaels (n 27), at 916, citing Josh Meyer &and Greg Miller, 'U.S. Secretly Tracks Global Bank Data', L.A. Times, 23 June 23, 2006, available at: <http://articles.latimes.com/2006/jun/23/nation/na-swift23>.

70 Id.

71 Michaels (n 27), at 917, citing Eric Lichtblau, 'Europe Panel Faults Sifting of Bank Data', N.Y. Times, 26 Sept. 26, 2006, available at: <http://query.nytimes.com/gst/fullpage.html?res=9F02EFDA1F31F935A1575AC0A9609C8B63&pagewanted=all>.

72 DOJ Memorandum to the Honorable James Orenstein, 11 Oct. 11, 2005 at 9, available at: <http://www.eff.org/file/filenode/USA_v_PenRegister/celltracking_govt_reply.pdf>.

73 See Christopher Soghoian, 'DOJ's 'hotwatch' Real-time Surveillance of Credit Card Transactions', Slight Paranoia Blog, 2 Dec. 2, 2010, <http://paranoia.dubfire.net/2010/12/dojs-hotwatch-real-time-surveillance-of.html>.

74 Id.

75 See *In Re Grand Jury Proceedings* (Bank of Nova Scotia), 740 F.2d 817 (11th Cir.), cert. denied, 469 U.S. 1106 (1985); *In Re Grand Jury Proceedings* (Bank of Nova Scotia), 691 F.2d 1384 (11th Cir. 1982), *cert. denied*, 462 U.S. 1119 (1983); *In Re Grand Jury Subpoena Directed to Marc Rich Company A.G.*, 707 F.2d 663 (2d Cir.), *cert. denied*, 463 U.S. 1215 (1983).

76 See eg *In Re Sealed Case*, 832 F.2d 1268, 1272–1274 (D.C. Cir. 1987) (explaining that subpoena for foreign company records is enforceable only if the company does sufficient business or otherwise has sufficient contacts within the United States to permit the court to exercise personal jurisdiction over it); *US v. The First Bank of Chicago*, 699 F.2d 341, 347(7th Cir.1983) (distinguishing the instant case from *Bank of Nova Scotia* because the foreign (Bahamian) law in that case was different from Greek law: disclosure with the consent of the customer would not be a criminal offence, and the power of a Bahamian court to permit disclosure did not appear to be as strictly limited).

office to persuade them to 'be patriots'.[77] Some of the information provided by Western Union following the exchange may have been disclosed via subpoenas, while some may have been provided though 'informal cooperation' rather than legal compulsion.[78] Since 9/11, Federal Express has also reportedly 'placed its databases at the government disposal' and 'demonstrated a willingness to open suspicious packages at the government's informal request (ie without a warrant)'.[79] Major airlines were also reported to have turned over extensive amounts of passenger data to the government because 'they thought they were obliged to do so'.[80] Third-party desire and willingness to cooperate with the government post-9/11 in the fashion described is understandable and, moreover, legal. Indeed, government outreach to establish good working relationships with industry is often necessary and desirable. But if entire industries (like supermarkets, hotels, travel agencies, etc.) routinely discloses information without minimal process, even when permitted under the law, then the government gets closer to achieving comprehensive awareness.

Current US legislative issues and conclusion

Legal standards and practices concerning the disclosure of third-party data to the government continue to be part of the privacy and security debates in Congress. A critical element of several cyber security bills, for example, is improved 'information sharing' between certain types of third parties and the government in the service of preventing cyber attacks, while, at the same time, appropriately limiting the type and amount of data shared to levels only necessary to achieve that purpose. Moreover, the government's continued desire for private-sector data can be seen in efforts to legislate third-party data retention requirements, as well as government interest in updating the Communications Assistance for Law Enforcement Act (CALEA). Congress is also considering ECPA reform, specifically with respect to new, more privacy protective standards for government access to location data and content communications stored 'in the cloud'. Notwithstanding efforts to expand and contract, or at least more specifically regulate government access to third-party data, the ongoing study of whether and how the government might acquire unmediated access to private-sector data must include a greater understanding of how the government interprets and uses its criminal and foreign intelligence authorities, including 'informal' government practices.

doi:10.1093/idpl/ips020
Advance Access Publication 26 August 2012

77 Michaels (n 27), at 914, citing Ron Suskind, *The One Percent Doctrine: Deep Inside America's Pursuit of Its Enemies Since 9/11* (pocket Books, 2006) 53–4.

78 Michaels (n 27), at 914, citing Suskind (n 77), at 231–33 and Robert Block, *Private Eyes: In Terrorism Fight, Government Finds a Surprising Ally: FedEx*, Wall St. J., 26 May 2005, available at: <http://online.wsj.com/article/0,,SB111707300196643763,00.html>.

79 Michaels (n 27), at 915, citing Block (n 78).

80 Michaels (n 27), at 928.