THE NSA PHONE CALL DATABASE: THE PROBLEMATIC ACQUISITION AND MINING OF CALL RECORDS IN THE UNITED STATES, CANADA, THE UNITED KINGDOM, AND AUSTRALIA

ANDREW P. MACARTHUR*

INTRODUCTION

The U.S. government historically has had broad authority to conduct foreign surveillance without a warrant to obtain information[1] to protect against national security threats.[2] However, the recent September 11, 2001 attacks have forced the government to recognize that threats to national security can and do occur from within the United States.[3] Thus, on occasion, the President has sanctioned domestic surveillance.[4]

---

* Andrew P. MacArthur received his J.D. from Duke University School of Law in 2007. Andrew was born in Canada and obtained his B.Sc. in Engineering from a Canadian university. At Duke Law School, Andrew served as an Executive Editor of the *Duke Journal of Comparative and International Law* (*DJCIL*). Andrew would like to thank the *DJCIL* staff for its help throughout the publication process.

1. *In re* Sealed Case No. 02-001, 310 F.3d 717, 742 (D.C. Cir. 2002) (stating that "all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information . . . . We take for granted that the President does have that authority [to conduct warrantless searches for foreign intelligence purposes].").

2. *Id.*; Susan Page, *NSA Secret Database Report Triggers Fierce Debate in Washington*, USA TODAY, May 11, 2006, *available at* http://www.usatoday.com/news/washington/2006-05-11-nsa-reax_x.htm [hereinafter Page, *NSA Secret Database*]; Richard A. Posner, Editorial, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31.

3. *See* Leslie Cauley, *NSA has massive database of Americans' phone calls*, USA TODAY, May 11, 2006, at 1A; Robert Block & Jay Solomon, *Pentagon Steps Up Intelligence Efforts Inside U.S. Borders*, CANDIDE'S NOTEBOOKS, Apr. 27, 2006, at A1, *available at* http://www.pierretristam.com/Bobst/library/wf-178.htm.

4. Dan Eggen, *Bush Authorized Domestic Spying*, WASH. POST, Dec. 16, 2005, at A1 (eavesdropping on domestic calls since 2002); Eric Lichtblau, *Bank Data Secretly Reviewed by U.S. to Fight Terror*, N.Y. TIMES, June 22, 2006, at A1.

In May 2006, *USA TODAY* reported that the National Security Agency (NSA) had created a database containing "tens of millions"[5] of domestic call records[6] obtained from various telecommunication providers.[7] The NSA then datamined[8] the records to detect possible terrorist threats against national security.[9] This Note analyzes the legality of the NSA call database.[10]

First, Part I discusses the factual background surrounding the NSA call database and the response from the President and the public. Part II looks at whether the government can legally collect call records without a warrant under the Foreign Intelligence Surveillance Act (FISA) and Pen Register Statute or alternatively using a National Security Letter (NSL). Part II also examines the telecommunication providers' liability under the 1996

---

5. John Diamond & Leslie Cauley, *Pre-9/11 Records Help Flag Suspicious Calling*, USA TODAY, May 22, 2006, at 6A. However, it has been alleged that the NSA has access to an AT&T call database containing 1.9 trillion call records. John Markoff, *Taking Snooping Further: Government Looks at Ways to Mine Databases*, N.Y. TIMES, Feb. 25, 2006, at C1. Relatively speaking, the 1.9 trillion call record database is small compared to some corporate databases such as Wal-Mart's. Kevin Maney, *Size of NSA's Database of Phone-Call Records isn't All That Impressive*, USA TODAY, May 16, 2006, at 3B.

6. Call records "are the electronic information that is logged automatically each time a call is initiated. For more than 20 years, local and long-distance companies have used call . . . records to figure out how much to charge each other for handling calls and to determine problems with equipment." Diamond & Cauley, *supra* note 5.

7. Cauley, *supra* note 3.

8. Datamining is defined as "the process of collecting large amounts of data from different sources . . . then searching for patterns within the data using computerized tools . . . with the goal of identifying significant relationships and predicting future trends and events." Matthew B. Stannard, *U.S. Phone-Call Database Ignites Privacy Uproar*, S.F. CHRON., May 12, 2006, at A1; Laura K. Donohue, *Criminal Law: Anglo-American Privacy And Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1144-45 (finding that the U.S. government has previously engaged in 199 datamining operations for various reasons "such as improving services, managing human resources, and detecting terrorist activity").

9. Cauley, *supra* note 3.

10. For a preliminary analysis of some of the legal issues discussed in this Note see Posting of Marty Lederman to Balkinization, http://balkin.blogspot.com/2006/05/further-thoughts-on-lawfulness-of.html (May 11, 2006, 10:08 PM); OrinKerr.com, More Thoughts on the Legality of the NSA Call Records Program, http://www.orinkerr.com/2006/05/12/more-thoughts-on-the-legality-of-the-nsa-call-records-program/ (May 12, 2006, 3:30 AM) [hereinafter Kerr, *More Thoughts*]; Posting of Kate Martin to ACS Blog, http://www.acsblog.org/bill-of-rights-guest-blogger-nsa-again-violates-the-law.html (May 11, 2006 4:26 PM); Posting of Orin Kerr to The Volokh Conspiracy, http://volokh.com/posts/1147361955.shtml (May 11, 2006, 12:13 PM) [hereinafter Kerr, *Thoughts*]; CTR. FOR DEMOCRACY & TECH., ILLEGAL NSA DATA MINING HIGHLIGHTS NEED FOR CONGRESSIONAL OVERSIGHT (2006), http://www.cdt.org/publications/policyposts/2006/8; The Online Newshour, *Legality of NSA Phone Program Questioned*, PBS, May 12, 2006, http://www.pbs.org/newshour/bb/law/jan-june06/privacy_05-12.html.

Telecommunications Act and 1986 Store Communications Act for voluntarily disclosing the records to the government.

Part III then asks whether datamining the obtained call records would constitute an unreasonable search under the Fourth Amendment. Part IV discusses possible defenses available to the government, such as the state secrets privilege and the President's authority (express and inherent) to bypass FISA. In Part V, the analysis shifts to the international stage and whether the NSA call database would be legal in Canada, the United Kingdom, and Australia, each of which strike a different balance between privacy rights and national security concerning the collecting and mining of call records than the United States.

I. BACKGROUND

On May 10, 2006, *USA TODAY* published a story alleging[11] that the NSA had created a secret[12] database containing "tens of millions"[13] of domestic call records with information such as the duration, date, and time of the call, and the caller and recipient's phone numbers.[14] However, the NSA's database neither contained the content of the call nor the customer's name or address.[15] The NSA, without a warrant, allegedly obtained the phone records from telecommunication providers such as AT&T and MCI[16] by setting up a "real time"[17] direct connection from the phone providers to the

11. Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006, at 2A [hereinafter Page, *Lawmakers*] (stating that President Bush has not "directly confirmed" the existence of the call database).

12. Page, *NSA Secret Database*, *supra* note 2. President Bush has stated that "appropriate members of Congress, both Republican and Democrat" were briefed about the program. *Id.* However, one member of Congress said "she hadn't been told all of the information included in the *USA TODAY* story. And all but a handful of lawmakers learned of the program for the first time in the news account." *Id.*

13. *See supra* note 5.

14. Diamond & Cauley, *supra* note 5 (stating that the NSA acquired the "number from which a call [was] made, . . . the number called; the route a call took to reach its final destination; the time, date and place where a call started and ended; and the duration of the call. The records also note whether the call was placed from a cellphone or from a traditional 'land line.'").

15. Page, *Lawmakers, supra* note 11.

16. *Id.*

17. Seymour M. Hersh, *National Security Dept. Listening In*, THE NEW YORKER, May 22, 2006, at 24 (stating that "[t]he N.S.A. is getting real-time actionable intelligence"). *See also* Texas A&M Glossary of Distance Education Terms, http://www.tamu.edu/ode/glossary.html (last visited Dec. 13, 2006) (defining "real time" as "[a]n application in which information is received and immediately responded to without any time delay").

NSA headquarters.[18] One carrier, Qwest, allegedly refused to grant the government access, citing concerns about the legality of the program without a warrant,[19] about who would have access to this data,[20] and how it would be used.[21]

After creating the database, the NSA allegedly datamined the call records for patterns or trends[22] of possible threats against national security.[23] For example, the NSA computers would flag calls to the United States coming from countries in the Middle East if the person receiving the call subsequently made a domestic call.[24] The NSA would then connect the flagged numbers to known phone numbers linked to terrorist activity.[25] After datamining the records, it is alleged that the NSA plans to keep the data indefinitely.[26]

President Bush has neither directly confirmed nor denied the existence of the NSA call database program.[27] However, President Bush has stated, in defending the wiretapping of international calls, that "one end of the [phone] communication must be outside the

18. Hersh, *supra* note 17 (stating that the telecommunication provider would setup a "high-speed circuit between its main computer complex and . . . [the] government-intelligence computer center"); Stephen Lawson, *Documents in AT&T Spying Case Unsealed*, MACWORLD, May 29, 2006, http://prisonplanet.com/articles/may2006/290506Documents.htm.

19. Cauley, *supra* note 3.

20. *Id.* (stating, "The NSA told Qwest that other government agencies, including the FBI, CIA and DEA, also might have access to the database . . . . The NSA regularly shares its information—known as 'product' in intelligence circles—with other intelligence groups.").

21. *Id.*

22. Alternatively, the call records could be used to assist in a wide range of investigations, such as by the police or government intelligence agencies. The NSA's New New Phone Database, http://www.radioopensource.org/the-nsas-new-new-phone-database/ (last visited Jan. 2, 2007). For example, assume the government believes that person X is a threat to national security. Instead of having to obtain a subpoena to get that person's phone records, the NSA could simply look up the person's name in the phone book or through other means, and obtain the person's number Y. Once the number Y is obtained, a government agency could then search the NSA call database for all calls made "to" and "from" that number Y. Moreover, the NSA is allegedly obtaining the real time data and the location of the call. *See* Diamond & Cauley, *supra* note 5. Thus, it could pinpoint a person's whereabouts in a matter of seconds after the call is made. *See* Velcro, Officials Spy on Calls, http://www.whatever.net.au/pipermail/velcro/2002-May/000090.html (May 1, 2002 16:30).

23. Cauley, *supra* note 3.

24. Diamond & Cauley, *supra* note 5.

25. *Id.*

26. CTR. FOR DEMOCRACY & TECH., *supra* note 10.

27. *See* Page, *Lawmakers*, *supra* note 11; *see also* Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 997 (N.D. Cal. 2006) (stating that the "court notes that despite many public reports . . . the government . . . *has never publicly disclosed* whether the NSA program reported by USA Today on May 11, 2006, actually exists") (emphasis added).

United States,"[28] leading most people to believe that only international calls—not domestic calls—were susceptible to surveillance.[29]

In addition to the President's response to the call database, the public has responded via public opinion polls and lawsuits. A *USA TODAY*/Gallup poll found that fifty-one percent of Americans disapprove of the program.[30] *USA TODAY* has also reported that as many as twenty class-action lawsuits have been filed in federal court against the government and telecommunication providers.[31]

II. DID THE NSA OBTAIN THE CALL RECORDS LEGALLY?

A. Foreign Intelligence and Surveillance Act

In 1975, a Congressional examination revealed that for at least twenty years the NSA had been intercepting international communications without a warrant at the request of various government agencies.[32] This revelation prompted the 1978 enactment of the Foreign Intelligence Surveillance Act (FISA),[33] which outlines the procedures that the government must follow to conduct electronic surveillance with or without a warrant.[34]

1. Electronic Surveillance. The first legal question is whether the acquisition of call records constitutes "electronic surveillance,"

---

28. Cauley, *supra* note 3.

29. *Id.*

30. Susan Page, *Poll: 51% Oppose NSA Database*, USA TODAY, May 14, 2006, http://www.usatoday.com/news/washington/2006-05-14-nsa-reax-poll_x.htm?POE=NEWISVA [hereinafter Page, *Poll*]. Two other polls have been taken by *Newsweek* and *The Washington Post*. David Jefferson, *Newsweek Poll: Americans Wary of NSA Spying Bush's Approval Ratings hit new lows as Controversy Rages*, MSNBC, May 14, 2006, http://www.msnbc.msn.com/id/12771821/site/newsweek/ (finding that fifty-three percent of people think the NSA call database is objectionable); *Washington Post-ABC News Poll*, WASH. POST, May 12, 2006, *available at* http://www.washingtonpost.com/wp-srv/politics/polls/postpoll_nsa_051206.htm (finding, in a poll taken before the *USA TODAY*/Gallup discussed in the text, that sixty-three percent consider the NSA call database an acceptable method to investigate terrorism). The *USA TODAY*/Gallup Poll may differ from the previous *Washington Post* poll in the way in which the question was asked, and additionally, the Gallup Poll includes more respondents and less margin of error. Page, *Poll*, *supra.*

31. Page, *Lawmakers*, *supra* note 11.

32. Cauley, *supra* note 3.

33. 50 U.S.C.S. §§ 1801-1811, 1821-1829, 1841-1846, 1861-1862, 1871 (LexisNexis 2006); *see also* Page, *Lawmakers*, *supra* note 11.

34. *See* Cauley, *supra* note 3; 50 U.S.C.S. § 1805(a) (LexisNexis 2006); 50 U.S.C.S. § 1802(a)(1)(A) (LexisNexis 2004).

which is defined[35] in § 1801(f)(1) as "the *acquisition* by an electronic . . . device . . . of the *contents* of any wire . . . *sent by* . . . a particular, known United States person who is in the United States."[36] Section 1801(n) defines "contents" as "any information concerning the *identity of the parties* to such communication or the *existence*, substance, purport, or meaning of that communication."[37] Thus, § 1801(n) broad definition covers more than merely the contents of a phone call and extends to the existence of the communication.[38]

Implicit in this definition of "electronic surveillance" is that the acquisition must occur in real time. In other words, the collection of historical records would not likely constitute "electronic surveillance."[39] The NSA is probably obtaining real time call records[40] as "[i]t does them no good to have [the telecommunication providers] back up the truck and unload the tapes. It needs a live feed from the server."[41] While it is true that the call records are missing customer identifiable information, such as the caller's name, the NSA could cross-reference those records in a matter of seconds to identify the persons to the communication. The fact that an extra step is required

35. The Senate Judiciary Committee (by a ten to eight vote) approved the National Security Surveillance Act of 2006 (also known as Senate Bill 2453). Source Watch, National Security Surveillance Act of 2006, http://www.sourcewatch.org/index.php?title=National_Security_Surveillance_Act_of_2006 (last visited Dec. 13, 2006). Senate Bill 2453 redefines, in § 701(4), "electronic surveillance" to only require a warrant when the program captures the substance of the communication. The Orator Network, S. 2453, http://www.theorator.com/bills109/s2453.html (last visited Dec. 13, 2006). Thus, the collection of call records by the NSA would probably not be considered electronic surveillance because the call records do not capture the substance of the communication. It is questionable whether the bill will be passed because the Democrats currently have control over both Houses.

36. 50 U.S.C.S. § 1801(f)(1) (LexisNexis 2006) (emphasis added).

37. 50 U.S.C.S. § 1801(n) (LexisNexis 2006) (emphasis added).

38. *Cf.* 18 U.S.C.S. § 2510(8) (LexisNexis 2002) (defining "contents" for criminal interception of electronic communications as "any information concerning the substance, purport, or meaning of that communication").

39. *See* Tom Brune, *Bush under fire for phone taps*, NEWS DAY, May 12, 2006, at A4 (stating that "[r]eal-time collection of data would require the NSA to get a warrant . . . [under the FISA, but] if the NSA is collecting historical records, the telecommunications companies face [potential liability under a different Act]"); *Bush Responds to USA TODAY Story Regarding NSA Database of Phone Calls,* TECH L. J. (May 11, 2006), http://www.techlawjournal.com/topstories/2006/20060511b.asp (distinguishing between real time and non-real time collection of data in analyzing the government's potential liability under FISA).

40. Hersh, *supra* note 17.

41. William Arkin et al., *Bush Defends Spying After NSA Database Report*, MSNBC, May 11, 2006, http://www.msnbc.msn.com/id/12734870/page/3/.

to identify the person should not allow the government to bypass FISA.

Notwithstanding that the call records do not identify the parties to the communication, the call records do prove that a communication took place and thus would confirm the "existence" of the communication in § 1801(n); accordingly, the NSA would be acquiring "contents" in § 1801(f)(1) and therefore conducting electronic surveillance within the meaning of FISA.

2. FISA Procedures. Even if the government is conducting electronic surveillance, FISA provides two possible procedures that could permit the surveillance. The first procedure[42] is not important from a legal perspective, as the NSA did not seek a warrant for the acquisition of call records.[43] But the decision is perplexing from a strategic perspective, as only five applications out of nineteen thousand have been refused by the Foreign Intelligence Surveillance Court[44] and the government's submission is *ex parte*.[45] The government most likely did not follow the first procedure, for it believed that the court would not approve a program of the size and scope of the NSA call database.[46] When it was enacted, FISA did not contemplate a program like the call database, which involves millions of people and possibly thousands of targets.[47] Moreover, the Bush administration finds the procedures of FISA too slow to react to the threat of terrorism.[48]

In addition to proceeding with a warrant, the President can conduct electronic surveillance without a warrant for one year, provided three conditions are met.[49] First, the electronic surveillance

---

42. *See* 50 U.S.C.S. § 1805(a) (LexisNexis 2006) (requiring five conditions be met to obtain a warrant for conducting electronic surveillance).

43. *See* background discussion *supra* Part I.

44. Electronic Frontier Foundation, ATT-NSA FAQ, http://www.eff.org/legal/cases/att/faq.php (last visited Dec. 13, 2006).

45. 50 U.S.C.S. § 1805(a) (LexisNexis 2006).

46. Page, *NSA Secret Database*, *supra* note 2; Cauley, *supra* note 3.

47. Posting of David Edwards to Veredictum, NSA Uses Private Firms for Massive Unchecked Domestic Surveillance, http://veredictum.com/node/109 (Feb. 27, 2006 12:44).

48. Cauley, *supra* note 3; *Revising FISA to Address 21st Century Threats to National Security: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 109th Cong. 2d sess. (2006) (testimony by Robert D. Alt, Fellow, The John M. Ashbrook Center for Public Affairs); Mort Kondracke, *NSA Data Mining Is Legal, Necessary, Sec. Chertoff Says*, REAL CLEAR POL., Jan. 20, 2006, http://www.realclearpolitics.com/Commentary/com-1_20_06_MK.html.

49. *See* 50 U.S.C.S. § 1802 (LexisNexis 2004).

must involve acquiring the "content of the communication" between foreign powers.[50] Second, the surveillance cannot "acquire the *contents* of any communication to which a United States *person*[51] is a party."[52] Finally, the surveillance must meet the "minimization procedures" defined in § 1801(h).[53] Under the first prong, it is unlikely that millions of people would be considered a foreign power. Next, and most important, the government appears to be acquiring the "contents" of a communication to which a citizen of United States is a party. Finally, prong three is unlikely to succeed because it is doubtful that the scope of the program meets the "minimization procedures"[54] required by FISA.

B. Pen Registers and Trap and Trace Devices

A pen register[55] records all the phone numbers dialed from a particular telephone, and a trap and trace device[56] records all numbers that dial a specific phone number.[57] There are two statutes that allow the use of a pen register or trap and trace device provided certain conditions are met.

Under the first statute, FISA,[58] these devices can only be used if the Attorney General certifies that "information likely . . . *is relevant to an ongoing investigation* to protect against international terrorism . . . provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."[59] This statute is unlikely

50. 50 U.S.C.S. § 1802(a)(1)(A) (LexisNexis 2004).

51. 50 U.S.C.S. § 1801(i) (LexisNexis 2006) (defining a "'United States person' . . . [as] a citizen . . . an alien lawfully admitted for permanent resident" and corporations incorporated in the United States).

52. 50 U.S.C.S. § 1802(a)(1)(B) (LexisNexis 2004) (emphasis added).

53. 50 U.S.C.S. § 1801(h) (LexisNexis 2006).

54. *Id.* (stating, in part, the government is required "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons").

55. A "pen register" is defined as "a device or process which records . . . dialing . . . information transmitted by an instrument." 18 U.S.C.S. § 3127(3) (LexisNexis 2001); 50 U.S.C. §1841(2) (2000).

56. A "trap and trace device" is "a device or process which captures the incoming electronic . . . impulses which identify the originating number." 18 U.S.C.S. § 3127(4) (LexisNexis 2001); 50 U.S.C. §1841(2) (2000).

57. Everything2, NSA phone record database, http://www.everything2.com/index.pl?node_id=1807359 (May 17, 2006, 6:38).

58. 50 U.S.C.S. §§1841-1846 (LexisNexis 2006).

59. 50 U.S.C.S. § 1842(c)(2) (LexisNexis 2006).

to apply because the acquisition of millions of records would not likely be relevant to an ongoing investigation; the government would not know if a person was a terrorist threat until it obtained the records and performed the necessary analysis.

The second statute, the criminal pen register,[60] prohibits both the use of a pen register or trap and trace device unless the court approves the device or an exception applies.[61] The telecommunication providers can use either device to obtain the call records under the operation and maintenance exception,[62] such as billing. However, if the NSA is obtaining real time call records from the phone providers, then it would be using the same device as the telecommunication providers, yet not meeting any of the exceptions such as maintenance and operation.

Alternatively, if the NSA did not acquire the call records in real time, it could be argued that the telecommunication providers legally collected the call records and then the NSA obtained these records without using any devices.[63] However, that argument would render the pen register statute meaningless,[64] as the NSA could circumvent the statute and obtain all the same information (such as phone numbers) that they would normally acquire through either the pen register and/or trap and trace device. Thus, it is difficult to reconcile how it is legal to acquire pen register information without a court order through the telecommunication providers, yet it is illegal to use a pen register without a court order to obtain the same information.[65]

C. National Security Letter as an Alternative to FISA

Under 18 U.S.C. § 2709, also known as the National Security Letter (NSL), the Federal Bureau of Investigation (FBI) can obtain[66]

---

60. 18 U.S.C.S. §§ 3121-3127 (LexisNexis 2002).

61. 18 U.S.C.S. § 3121(a)-(b) (LexisNexis 2001).

62. *See* 18 U.S.C.S. § 3121(b) (LexisNexis 2001).

63. *See* Kerr, *Thoughts*, *supra* note 10.

64. *See id.*

65. Legal Issues Governing the Administration's Newly Disclosed Surveillance Program, Unclaimed Territory, http://glenngreenwald.blogspot.com/2006/05/legal-issues-governing-administrations.html (May 11, 2006, 1:34).

66. The FBI is issuing more than thirty thousand NSLs per year. Robyn E. Blumner, *National Security Letters Put Privacy at Risk*, ST. PETERSBURG TIMES, Nov. 11, 2005, at 5P; Christopher P. Raab, iBrief, *Fighting Terrorism in an Electronic Age: Does the PATRIOT Act Unduly Compromise Our Civil Liberties?*, 2006 DUKE L. & TECH. REV. 0003 ¶ 26 (2006) (stating that "the FBI issues more than 30,000 NSLs yearly, a number that the Justice Department would neither confirm nor deny").

records without a warrant if the "records sought are relevant to an authorized investigation to protect against international terrorism."[67] Further, the recipient of an NSL is prohibited from disclosing the fact that the government made the request.[68]

An interesting legal issue is whether the NSA could have the FBI obtain the call records using a NSL and then share[69] that information with the NSA, thus avoiding the requirements of FISA.[70] The answer is likely no. The FBI usually conducts targeted investigations of individual suspects based on known facts.[71] Thus, Congress did not contemplate giving the FBI authority to make broad, indistinguishable requests for numerous records without any individualized suspicion.[72] Section 2709(b)(1) prohibits any investigation based on activities protected by the First Amendment;[73] the collection of phone records could be seen as violating that clause because the NSA is collecting data based on phone conversations.[74] Finally, an NSL "is an administrative subpoena,"[75] meaning that the subpoena must be relevant, limited, and specific enough to avoid being too burdensome.[76] The request by the FBI for the call records would not meet any of these conditions because the request would be for all call records without any suspicion of terrorist activity.

D. Telecommunication Providers' Liability

The 1996 Telecommunications Act states that "[e]very telecommunications carrier has a duty to protect the confidentiality of proprietary information... relating to... customers."[77] This customer proprietary network information (CPNI) has been defined

67. 18 U.S.C.S. § 2709(b)(1) (LexisNexis 2006).

68. *See* 18 U.S.C.S. § 2709(c) (LexisNexis 2006).

69. Cauley, *supra* note 3.

70. The FBI could also use something similar to an NSL called the "library records provision" (LRP) under 50 U.S.C.S. § 1861 (LexisNexis 2006). Blumner, *supra* note 66. In contrast to the NSL, which does not require any judicial oversight, the LRP would require *ex parte* court approval before any records could be obtained. 50 U.S.C.S. § 1861(c) (LexisNexis 2006). Thus, the LRP requires at least one more step before any records can be acquired.

71. Martin, *supra* note 10.

72. *Id.*; *see also* 18 U.S.C.S. § 2709(b)(1) (LexisNexis 2006) (stating that the FBI can obtain records "of *a person* [not millions of persons] or entity") (emphasis added).

73. *See* 18 U.S.C.S. § 2709(b)(1) (LexisNexis 2006).

74. Lederman, *supra* note 10.

75. Doe I v. Gonzales, 449 F.3d 415, 417 (2d Cir. 2006).

76. Donovan v. Lone Steer, Inc., 464 U.S. 408, 415 (1984); *see* Lederman, *supra* note 10.

77. 47 U.S.C. § 222(a) (2000).

as "information that relates to the quantity, technical configuration, type, destination, and amount of use of a telecommunications service subscribed to by any customer."[78]

The first question is whether the call records' details, such as duration, timing, and phone numbers,[79] acquired by the NSA constitute CPNI. The Federal Communications Commission has recently stated that "CPNI includes information such as the *phone numbers called* by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer, such as call waiting. CPNI therefore includes highly-sensitive personal information."[80] Thus, it is likely that the telecommunication providers were prohibited from disclosing the call records to the government unless the customer consented, required by law,[81] related to billing, to prevent fraud, and one of a few other exceptions was present.[82]

The government could argue that the consumer has consented[83] to the disclosure through the standard phone contract or alternatively, that the government coerced the phone providers to supply those records.[84] The problem with the first argument is that any disclosure provision in the contract would likely be voided based on public policy concerns or violating the spirit of the Telecommunications Act. Further, according to 47 C.F.R. § 64.2007, a customer can always revoke his or her approval,[85] and this would be likely once the customer learns how his or her information is being used. The second argument is weaker as it appears the

78. 47 U.S.C. § 222(h)(1)(A) (2000); Leah E. Capritta, *Tenth Circuit Survey: Communications Law: U.S. West, Inc. v. FCC Interprets the First Amendment Ramifications of "Customer Proprietary Network Information,"* 77 DENV. U.L. REV. 441, 442 (2000) (quoting California v. FCC, 39 F.3d 919, 930 (9th Cir. 1994)) (stating that "CPNI is information about a telephone customer's use of the telephone network, such as the number of lines ordered, service location, type and class of services purchased, usage levels, and calling patterns").

79. Diamond & Cauley, *supra* note 5.

80. *In Re* Telecommunications Act of 1996, 21 FCC Rcd 1782, 1784 (2006) (emphasis added).

81. 47 U.S.C. § 222(c)(1) (2000).

82. *See* 47 U.S.C. § 222(d)(1)-(4) (2000).

83. *See* 47 C.F.R. § 64.2007(a) (2007) (stating that a phone provider can obtain customer consent to use customer proprietary network information "through written, oral or electronic methods").

84. Talk Left, NSA Phone Records: What's the Problem?, http://www.talkleft.com/story/2006/05/13/892/21491 (May 13, 2006, 12:16:07 PM EST).

85. *See* 47 C.F.R. § 64.2007(a)(2) (2007).

telecommunication providers had a voluntary agreement with the government.[86]

In addition to the Telecommunications Act, the 1986 Stored Communications Act (SCA) (codified at 18 U.S.C. § 2702) states that "a provider of remote computing service or electronic communication[87] . . . shall not knowingly divulge a record . . . pertaining to a subscriber . . . to any governmental entity."[88] There are six potential exceptions in § 2702(c), including consent by the customer and emergency (death or serious injury).[89] Before addressing consent, it is unlikely that the disclosure of call records is necessary to avoid immediate death or serious injury[90] as the call database was enacted to identify future terrorist threats.

The consent exception is not likely to succeed because the First Circuit, in construing consent in an analogous statute,[91] gave it a narrow meaning. The court "emphasize[d] that 'consent should not

86. *See* background discussion *supra* Part I.

87. It may be possible to argue that the telecommunication providers are long-distance carriers and thus not providers of electronic communication service as defined in § 2510(15). OrinKerr.com, New Facts Suggest A Possible Reason Why the Phone Companies May Not Be Liable For the NSA Call Records Program, http://www.orinkerr.com/2006/05/18/new-facts-suggest-a-possible-reason-why-the-phone-companies-may-not-be-liable-for-the-nsa-call-records-program (May 18, 2006, 1:30 PM) [hereinafter Kerr, *New Facts*].

88. 18 U.S.C.S. § 2702(a)(3) (LexisNexis 2006). Section 2702(a)(1) and (a)(2) do not apply because the telecommunication provider is not disclosing "contents." Section 2711 states, "As used in this chapter . . . the terms defined in § 2510 of this title . . . have, respectively, the definitions given such terms in that section." 18 U.S.C.S. § 2711(1) (LexisNexis 2006). Section 2510 defines "contents" as any "electronic communication . . . concerning the substance, purport, or meaning of that communication." 18 U.S.C.S. § 2510 (LexisNexis 2002). Thus, call records' details would likely not fit within this definition because the phone conversation contents are not being transferred to the NSA.

89. Disclosure is also permitted when (1) authorized by § 2703; (2) a necessary part of service; (3) "connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990"; (4) any person not a government entity. 18 U.S.C.S. § 2702(c) (LexisNexis 2006). The only possible disclosure exception that could apply is the "authorized by section 2703" exception. Section 2703(c) permits disclosure when the government obtains a warrant, obtains a court order, obtains consent, is enforceing laws against telemarketing fraud, or is using an administrative subpoena. 18 U.S.C. § 2703(c) (LexisNexis 2006). It is unlikely that § 2703's first four exceptions apply. As for its fifth exception, it is also unlikely as the NSA might not have administrative subpoena power and even if it did, there is no evidence that it was issued. Imjtk, Your Telco owes you $1,000, http://imjtk.com/your-telco-owes-you-1000.php (May 14, 2006); s*ee generally*, Lederman, *supra* note 10 (stating that "there appears to have been no such administrative subpoena here").

90. Kerr, *Thoughts*, *supra* note 10.

91. *Id.* (stating, "There are no cases interpreting [exactly] . . . what consent means in 2702(c)(2), but like many of the exceptions in the SCA it is clearly a copy of an analogous exception in the close cousin of the SCA, the federal Wiretap Act . . . .").

casually be inferred,' . . . particularly in a case of deficient notice. The surrounding circumstances must convincingly show that the party knew about and consented to the interception in spite of the lack of formal notice or deficient formal notice."[92] Thus, because the customers likely had no notice of the transfer of call records, it is doubtful that the customers consented to the records being disclosed by the phone providers.

Even if the government applied for a court order after obtaining the records without meeting one of the exceptions to validate the transfer, it is likely that the request would be denied.[93] In one case, a carrier provided the government with records voluntarily and the government then applied for a court order afterwards to retroactively validate the transfer.[94] In denying the government's request for an order, the court held that the government was required to obtain an order *before* the telecommunication provider disclosed the records.[95]

Finally, an argument could be made that the SCA only prohibits the disclosure of stored records as opposed to records acquired in real time.[96] A Federal District Court noted, "As implied by its full title ('Stored Wire and Electronic Communications and Transactional Records Access'), the entire focus of the SCA is [on] . . . *existing communications* . . . ."[97] This conclusion is based on that fact that there are procedural protections in other statutes permitting real time surveillance that are absent in the SCA.[98] Unlike both the Pen Register Statute and Wiretap Act, the SCA's law enforcement

92. United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995) (citation omitted).

93. *See In re* Application of U.S. For a Nunc Pro Tunc Order For Disclosure of Telecommunications Records, 352 F.Supp.2d 45 (D. Mass. 2005).

94. *Id.* at 46.

95. *See id.*

96. *In re* Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification Sys. on Tele. Nos. [sealed] and [sealed] and the Prod. of Real Time Cell Site Info., 402 F. Supp. 2d 597, 600 (D. Md. 2005); *In re* Application of the U.S. for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Tel. Nos. [sealed] and [sealed], 416 F. Supp. 2d 390, 395 (D. Md. 2006) (stating, "The structure of the SCA shows that the statute does not contemplate orders for prospective [or real time] information.").

97. *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 459 (S.D.N.Y. 2006) (quoting *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005)) (emphasis added).

98. *Id.* (emphasis added); *In re* Orders Authorizing Pen Registers and Caller Identification Devices, 416 F. Supp. 2d at 395 n.7. (stating, "The SCA regulates access to records and communications in storage and therefore lacks provisions typical of prospective [or real time] surveillance statutes.").

surveillance is not limited in length by a court order and the order is not required to be automatically sealed to maintain secrecy of the surveillance.[99] Thus, if Congress intended the SCA to cover real time disclosure of records then it would have included in the SCA similar real time provisions.[100]

In contrast, another court has found that because the SCA has no express limitation on the disclosure of real time data, that the SCA covers both the disclosure of stored and real-time records.[101] Moreover, even if the SCA only covers stored records, it is possible to argue that the records will be stored, if only briefly, by the phone providers before transferring those records to the NSA; accordingly, the phone providers would be violating the SCA by disclosing those stored records.[102] The better-reasoned of the two arguments is that the real time disclosure of call records would not violate the SCA unless historical records were disclosed. This is based on the fact that the SCA is missing the same structural characteristics as other real time statutes and a momentary storage of call records should not count as a stored record under the SCA.

III. DID THE GOVERNMENT VIOLATE THE FOURTH AMENDMENT BY DATAMINING THE CALL RECORDS?

The Fourth Amendment protects the "[t]he right of the people . . . against unreasonable searches."[103] A challenge based on the Fourth Amendment requires that a person can claim "a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[104] The reasonable expectation of privacy analysis asks first, does the person have an actual (subjective) privacy expectation, and second, does society (objectively) consider the person's privacy expectation reasonable.[105] If the person meets both prongs of this test or establishes a legitimate privacy expectation, then the court must decide whether the intrusion is

99. *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d at 459.

100. *Id.*

101. *Id.*

102. *Id.*

103. U.S. CONST. amend. IV.

104. Smith v. Maryland, 442 U.S. 735, 740 (1979); Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. TECH. L. REV. 61, 71 (1999-2000).

105. *Smith*, 442 U.S. at 740; Skok, *supra* note 104, at 71.

reasonable.[106] The reasonableness of the search is based on the meaning of the Amendment at the time it was framed[107] or, if that yields no result, through a balancing test that weighs the private interest against the government interest.[108]

A. Prong One: Individual Reasonable Expectation of Privacy

Both *United States v. Miller*[109] and *Smith v. Maryland*,[110] decided in a span of three years, indicate that a person does not have a legitimate expectation of privacy in records that are voluntarily conveyed to a third-party. In *Miller*, the issue was whether the government violated the Fourth Amendment by requiring a bank to copy and inspect a person's records.[111] The Court held that a person had no reasonable expectation of privacy in information held by the third-party bank.[112] Similarly, in *Smith*, the issue was whether the government had performed a search under the Fourth Amendment[113] when a phone company, at the government's request, installed a pen register to record the numbers dialed.[114] The Court held that the person had no privacy expectation in the dialed numbers because those numbers are necessarily conveyed to the phone providers.[115]

However, *Miller* and *Smith* fail to consider how the Fourth Amendment has been altered over time with changing technology. For example, in *Olmstead v. United States*,[116] the Court initially held that no warrant was required to tap a phone line,[117] but later, in *Katz v. United States*,[118] the Court held that public conversations monitored by the government violated the Fourth Amendment.[119] The *Katz* approach could be viewed as "embrac[ing] whatever rules are needed

106. Skok, *supra* note 104, at 71.
107. *Id.* at 71-72.
108. *Id.*
109. 425 U.S. 435 (1976).
110. 442 U.S. at 735.
111. *Miller*, 425 U.S. at 439-40.
112. *See id.* at 444-45.
113. *Smith*, 442 U.S. at 738.
114. *Id.* at 737.
115. *Id.* at 742.
116. 277 U.S. 438 (1928).
117. *Id.* at 466 (holding that "the wire tapping here disclosed did not amount to a search or seizure within the meaning of the Fourth Amendment").
118. 389 U.S. 347 (1967).
119. *Id.* at 358-59.

to protect privacy against new technologies."[120] Moreover, recently in *Kyllo v. United States*,[121] the Court held that infrared searches of a person's home violate the Fourth Amendment.[122] However, *Kyllo* could be read as emphasizing the sanctity of a person's home,[123] rather than enhancing Fourth Amendment protections against new technologies.[124] The Court did state, though, in *Kyllo* that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[125] Thus, *Katz* and *Kyllo* could indicate that courts[126] will not ignore NSA's technology searching capabilities, especially considering that the NSA has "the *largest computing power* concentrated at any one place in the *whole world*."[127]

Another possible argument against *Miller* and *Smith* is that after both cases were decided Congress enacted statutes to protect the privacy of the records in each case. For example, after *Miller* and *Smith* were decided, Congress enacted The Right to Financial Privacy Act and Pen Register Act respectively.[128] Moreover, since *Miller* and *Smith* were decided, Congress has enacted the 1996 Telecommunications Act and 1986 Store Communications Act to

120. Orin S. Kerr, *The Fourth Amendment and new Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 818 (2004) [hereinafter Kerr, *Fourth Amendment*].

121. 533 U.S. 27 (2001).

122. *Id.* at 40.

123. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 536-38 (2005) [hereinafter Kerr, *Searches and Seizures*].

124. *See* Kerr, *Fourth Amendment*, *supra* note 120, at 835; *but see Katz*, 389 U.S. at 359 (stating that Fourth Amendment "considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of [an outside place] . . . . Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

125. *Kyllo*, 533 U.S. at 33-34.

126. Patricia L. Bellia, *The Fourth Amendment and Emerging Communications Technologies*, IEEE SEC. & PRIVACY, May/June 2006, at 20-28, *available at* http://www.computer.org/portal/site/security/menuitem.6f7b2414551cb84651286b108bcd45f3/index.jsp?&pName=security_level1_article&TheCat=1015&path=security/2006/v4n3&file=bellia.xml& (stating that "conclusions as to when an expectation of privacy is 'reasonable,' always difficult for judges to make, are especially difficult with evolving technologies").

127. Edwards, *supra* note 47 (quoting James Risen, *Tim Russert Show* (CNBC television broadcast, February 25, 2006)) (emphasis added). The Court in *Kyllo* based its holding, in part, on the fact the government used technology "not in general public use." *Kyllo*, 533 U.S. at 40. Similarly, it is likely that the NSA has technology that is not publicly available to facilitate the searching of call records.

128. Kerr, *Fourth Amendment*, *supra* note 120, at 855; Fred H. Cate, *Legal Standards for Data Mining*, HUNTON & WILLIAMS 13 (August 19, 2005), *available at* http://www.hunton.com/files/tbl_s47Details/FileUpload265/1250/Cate_Fourth_Amendment.pdf.

protect customer phone records from unauthorized disclosure.[129] Thus, taken as a whole, these statutes enacted by Congress indicate that records released to a third-party have some constitutional privacy value.

B. Prong Two: Societal Expectation of Privacy

Even after establishing the first prong, society would still have to recognize the expectation as reasonable. This second prong would face similar arguments as the first: namely, that society is not prepared to recognize a privacy right in information voluntarily disclosed to third parties. However, unlike both *Miller* and *Smith*, here public opinion polls indicate that at least fifty-one percent of society objects to the call database.[130] Also, at least twenty class-action lawsuits have been filed against the government and telecommunication providers, demonstrating society's displeasure with the disclosing and mining of call records.[131] Thus, society may one day be willing to recognize a privacy expectation in third-party records that it was not prepared to recognize during the era of *Miller* and *Smith*.

C. Reasonableness of the Search

Some commentators believe that a computer cannot perform a "search" within the meaning of the Fourth Amendment.[132] Judge Richard Posner, for example, has stated that "processing of data cannot . . . invade privacy. . . . This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer."[133] Another leading Fourth Amendment scholar has advocated the "exposure-based approach," in which data is not search until it "is exposed to human observation."[134]

---

129. *See generally*, Lederman, *supra* note 10 (reasoning that "Smith v. Maryland is based on the idea that phone users do not have a legitimate, reasonable expectation of privacy in who they call. However, the fact that laws like the stored communications act . . . and other privacy laws now exist give people a reasonable expectation of privacy in that information").

130. *See* background discussion *supra* Part I.

131. *Id.*

132. *See generally* Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83 (2006).

133. Posner, *supra* note 2.

134. Kerr, *Searches and Seizures*, *supra* note 123, at 547-48.

No perfect datamining program exists, and thus human eyes will eventually view the data, resulting in a search that implicates the Fourth Amendment.[135] Additionally, in the binary world, the NSA could possibly perform a significant number of searches[136] in what would take the police a lifetime to perform in the physical world. Moreover, unlike the physical world, where any search conducted would require probable cause,[137] the binary world has no judicial oversight or statutory procedures to follow[138] and consequently there is a greater chance for abuse of power.[139] Further, unlike in the physical world, the person in the binary world would have no notice[140] that a search was even performed.[141] Because there is no notice, a person could not deter the government through voting or political pressure or even "regulate their behaviour to avoid unwanted intrusions."[142] Thus, datamining should be considered a search and be examined for reasonableness by balancing the government and private interests.[143] Mining a database so large lacks reasonableness

135. Zittrain, *supra* note 132, at 92.

136. *See* Kerr, *Searches and Seizures*, *supra* note 123, at 534 (stating that "computer searches involve entire virtual worlds of information").

137. United States v. Abboud, 438 F.3d 554, 571 (6th Cir. 2006).

138. Zittrain, *supra* note 132, at 91.

139. *See* United States v. U.S. Dist. Ct., 407 U.S. 297, 316-17 (1972); *see also* 4&20 Blackbirds, Data Mining May be Legal—But is Still Repugnant, http://4and20blackbirds.wordpress.com/2006/05/12/data-mining-may-be-legal-but-is-still repugnant/ (May 12, 2006, 5:55) [hereinafter Blackbirds].

140. In the physical world, even with a search warrant the police are required, in most cases, to "knock and announce" before entering a house. Wilson v. Arkansas, 514 U.S. 927, 934 (1995); *but see* Hudson v. Michigan, 126 S. Ct. 2159, 2168 (2006) (holding that violating the "knock and announce" rule will not result in the evidence being suppressed). Thus, some notice is even required by officers before executing a search warrant on a home. In contrast, the binary or digital world requires none even without a search warrant. While it is true that the "knock and announce" rule is specific to the home, the purpose of the rule was to prevent destruction of property and avoid violence just like providing notice to owners of the call records could prevent the potential suspects from acting violently or destroying important evidence relating to national security. *Id.* at 2165.

141. Zittrain, *supra* note 132, at 91-92; Blackbirds, *supra* note 139.

142. Gus Hosein et al., *Invasive, Illusory, Illegal, and Illegitimate: Privacy International and EDRi Response to the Consultation on a Framework Decision on Data Retention*, Privacy International, Sept. 15, 2004, http://www.privacyinternational.org/issues/terrorism/rpt/responsetoretention.html.

143. Reasonableness could not be determined based on when the Amendment was framed because computer searching did not exist when the Fourth Amendment was enacted. Vernonia Sch. Dist. 47j v. Acton, 515 U.S. 646, 652-53 (1995) (quoting Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 619 (1989)) (citations omitted) ("[W]here there was no clear practice, either approving or disapproving the type of search at issue, at the time the constitutional provision was enacted, whether a particular search meets the reasonableness

because it is inefficient, that is, many false positives are going to occur, resulting in innocent people being jailed or suffering reputational harm.[144]

IV. GOVERNMENT'S DEFENSES

A. State Secrets Privilege

The state secrets privilege is a rule of evidence that makes inadmissible any material detrimental to national security.[145] The privilege can be invoked on two grounds. First, if there is a covert espionage agreement with the government, then the court is categorically barred (also known as the *Totten* bar) from hearing the case.[146] Second, if there is no categorical bar, then the court determines (1) if the state secrets privilege has been properly asserted, and (2) whether disclosure would be reasonably dangerous to national security.[147]

The government is likely to argue that the *Totten* categorical bar applies and ends the judicial inquiry, but this argument is misplaced. The basis for this argument would be that the government and the phone providers have an agreement in place,[148] analogous to a covert espionage agreement. However, implicit in *Totten* was that one who makes a covert agreement agrees not to disclose the agreement, even if breached.[149] But, any potential challenger to the NSA call database program would likely be a consumer who is not part of the government-phone provider agreement and thus would not be "bound by any implied covenant of secrecy."[150] Further, *Totten* is

---

standard 'is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'").

144. Stannard, *supra* note 8 (stating that "the problem with applying data mining techniques to terrorism . . . is that terrorism is so rare, and the databases being mined are so large, that false positives are inevitable and often more common than truly accurate results. And unlike using data mining to spot credit card fraud, where at most a false positive triggers a worried call from Visa to a cardholder and perhaps a temporary suspension of the card's use, a false positive in a terror investigation can put an innocent person in jail.").

145. Hepting v. AT&T Corp., 439 F. Supp.2d 974, 980 (N.D. Cal. 2006).

146. *See id.* at 980-81 (citing Totten v. United States, 92 U.S. 105, 106 (1876)).

147. *Id.* at 981-82 (citing United States v. Reynolds, 345 U.S. 1, 7-8 (1953)).

148. *See* Cauley, *supra* note 3 (stating that "three telecommunications companies [AT&T, BellSouth, and Verizon] are working under contract with the NSA."); *but see* Page, *Lawmakers*, *supra* note 11 (providing an update stating that "the newspaper cannot confirm that BellSouth or Verizon contracted with the NSA to provide bulk calling records to that database").

149. *Hepting*, 439 F. Supp.2d at 991.

150. *Id.* at 991.

inapplicable here because it would result in the plaintiff's case being dismissed "based solely on the government's conclusory statements without any real judicial review."[151]

In contrast to the *Totten* categorical bar, the government can likely assert the state secrets privilege under the second ground, as both conditions are likely met. It likely has asserted the privilege correctly,[152] and there have been no public disclosures meaning that any future disclosures could potentially be dangerous to national security.[153] The court in *Hepting v. AT&T Corp.*[154] agreed that both conditions were met, and the privilege applies. However, the court reluctantly reached this conclusion because NSA public disclosures about other security programs may have alerted any potential terrorists to the call database.[155] In fact, the court even warned that if any public disclosures occurred accidentally or deliberately later on, then those disclosures might preclude the government from asserting the state secrets privilege.[156]

B. The President's Authority to Bypass FISA

1. Government's Arguments. The President could first argue that he has express authority to override the FISA procedures and create the NSA call database. Section 1809(a)(1) provides that any electronic surveillance "authorized by statute" is exempt from the FISA procedures.[157] The Authorization for the Use of Military Force (AUMF)[158] could provide such authorization, as it states that the

151. Terkel v. AT&T Corp., 441 F. Supp.2d 899, 908 (N.D. Ill. 2006); *see also* Hamdi v Rumsfeld, 542 U.S. 507, 536 (2004) (plurality opinion) (stating, "Whatever power the United States Constitution envisions for the Executive in its exchanges with other nations or with enemy organizations in times of conflict, it most assuredly envisions a role for all three branches when individual liberties are at stake.").

152. The Supreme Court has held that to properly assert the state secrets privilege there must be "[1] formal claims of privilege, [2] lodged by the head of the department which has control over the matter, [3] after actual personal consideration by that officer." United States v. Reynolds, 345 U.S. 1, 7-8 (1953). All the requirements are likely to be met here.

153. *See Hepting*, 439 F. Supp.2d at 991, 997-98 (allowing the state secrets privilege based on the lack of any public disclosures); *Terkel*, 441 F. Supp.2d at 901 (stating that "there have been no public disclosures of the existence or non-existence" of the call database).

154. 439 F.Supp.2d at 991.

155. *Id.* at 997.

156. *Id.* at 991, 997-98.

157. 50 U.S.C. § 1809(a)(1) (2000).

158. Authorization for Use of Military Force, Pub. L. No. 107-40, § 2, 115 Stat. 224, 224 (2001). Also see the joint resolution to authorize the use of military forces in Iraq, which states that the "President is authorized to use the Armed Forces of the United States as he determines

President is to "use all necessary and appropriate force . . . to prevent any future acts of . . . terrorism against the United States."[159]

Secondly, the President could argue that the Supreme Court, in *Hamdi v. Rumsfeld*,[160] held that government action that is a "fundamental incident of waging war" is authorized by the AUMF's "necessary and appropriate force" clause.[161] Because intelligence gathering is a significant part of combat, the NSA's collection and mining of call records to prevent terrorist threats would be authorized by the AUMF's force clause.[162] Third, and finally, it could also be argued that the Constitution provides the President with inherent authority to bypass FISA and create the NSA call database.[163]

2. Analysis. The first argument that the AUMF overrides FISA is not supported by FISA's text, which states that FISA "shall be the *exclusive means* by which electronic surveillance . . . may be conducted."[164] One court has stated that the exclusivity language "makes it impossible for the President to 'opt-out' of the legislative scheme."[165] It is a settled canon of statutory interpretation that general provisions are superseded by specific provisions.[166] FISA does not permit domestic electronic surveillance without a warrant, but the AUMF allows the President to use all "necessary and appropriate

---

to be necessary and appropriate in order to . . . defend the national security of the United States against the continuing threat posed by Iraq" as another possible source of express congressional authority. Authorization for Use of Military
Force Against Iraq Resolution of 2002, Pub. L. No. 107-243, § 3, 116 Stat. 1498, 1501 (2002).

159. Authorization for Use of Military Force, § 2.

160. 542 U.S. 507 (2004).

161. *Id.* at 519; Memorandum from Elizabeth B. Bazen & Jennifer K. Elsea, Legislative Attorneys, Cong. Research Serv., on Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information, (Jan. 5, 2006) (available at http://leahy.senate.gov/issues/Eavesdropping/CRS%20report%20Jan%205%202006.pdf) [hereinafter Congressional Research Service].

162. This type of authority could be called "modified-express" because the President would have express authority from Congress, but only for actions that are a "fundamental incident of waging war."

163. U.S. CONST. art. II, § 1(stating that "the executive power shall be vested in a President"); U.S. CONST. art. II, § 2 (stating that "the President shall be Commander in Chief of the Army and Navy.").

164. 18 U.S.C.S. §2511 (2)(f) (LexisNexis 2002) (emphasis added).

165. United States v. Andonian, 735 F. Supp. 1469, 1474 (C.D. Cal. 1990), *aff'd in part and remanded,* 29 F.3d 634 (9th Cir. 1994), *cert. denied*, 513 U.S. 1128 (1995).

166. PresstheNews.Com, The NSA Wiretap Program Violates FISA, and the Constitution's Separation of Powers Clauses, http://www.pressthenews.com/wt3.htm (last visited Dec. 14, 2006) [hereinafter The NSA Wiretap Program].

force."[167] Thus, it would take a strained reading to find that the AUMF's general provision overrides FISA's specific language[168] requiring a warrant for domestic surveillance. Notwithstanding FISA's text, it is unlikely that gathering and datamining numerous call records constitutes the "necessary and appropriate force" required to invoke the AUMF. [169]

Similarly, the second argument for Presidential authority, relying on *Hamdi*, is also misplaced. While it is true that intelligence acquisition is an important part of any combat, "it is not clear that the collection of intelligence constitutes a use of force."[170] In *Hamdi*, the Court held that the AUMF authorized the detention of a United States citizen even though the Non-Detention Act provided that a United States citizen could not be detained unless Congress authorized it.[171] Justice O'Connor, writing for the plurality of the court, found that the AUMF does not support "indefinite detention for the purpose of interrogation."[172] Thus, the Court seemed to be indicating that intelligence gathering is not a necessary or appropriate force. Accordingly, because the NSA call database is for intelligence purposes, it would likely not constitute the use of force authorized by the AUMF's "necessary and appropriate force" clause.

Third, the argument that the President has inherent authority is also unlikely to succeed. When President Carter signed FISA into law, he stated that the bill "clarifie[d] the Executive's authority to gather foreign intelligence by electronic surveillance in the United States."[173] Thus, even the President responsible for approving FISA acknowledged that FISA limits the President's authority to conduct electronic surveillance.[174] While it could be argued that the President's authority is heightened during a time of conflict, the

167. *Id.*

168. *See id.*

169. *See* Congressional Research Service, *supra* note 161.

170. *Id.*

171. Hamdi v. Rumsfield, 542 U.S. 507, 519 (2004).

172. *See id.* at 521.

173. Letter from the Ctr. For Constitutional Rights to the Senate Intelligence Comm. (May 17, 2006) (available at http://www.ccr-ny.org/v2/reports/report.asp?ObjID=5hgZvLHaDC&Content=776).

174. Additionally, it could be argued that when Congress amended FISA in 2001, a month after the AUMF was adopted, it implicitly recognized that the AUMF does not bypass FISA. Posting by Orin Kerr to The Volokh Conspiracy, http://volokh.com/posts/1135029722.shtml (Dec. 19, 2005, 4:02 PM) [hereinafter Kerr, *Legal Analysis*]; The NSA Wiretap Program, *supra* note 166.

Court in *Hamdi* stated that "a state of war is not a blank check for the President" and that all three branches should be involved when civil liberties are at stake.[175] Thus, *Hamdi* indicated that the President's inherent authority is circumscribed even during a time of war.

V. WOULD THE CALL DATABASE BE LEGAL IN CANADA, THE UNITED KINGDOM, AND AUSTRALIA?

An analysis of the NSA call database under Canadian, British, and Australian law could provide[176] insight into American law and how to improve it,[177] especially considering the degree to which privacy rights vary from country to country.[178] For example, Privacy International, a privacy watchdog group,[179] ranked Canada as having "significant protections and safeguards."[180] It ranked Australia and the United Kingdom as having "systemic failure to uphold safeguards" and an "endemic surveillance societ[y]," respectively,[181] while the United States received an "[e]xtensive surveillance societ[y]" ranking. This indicates that much can be learned by evaluating the collection and mining of call records and the balances

175. *Hamdi*, 542 U.S. at 536.

176. One scholar has evaluated the NSA call database, in general, under both German and French law and concluded that the NSA call database would be illegal in both countries. This conclusion was based, in part, on the fact that (1) the government would have access to a significant amount of data; (2) the government would hold the data for a long period of time; (3) citizens would have no ability to determine how their data is being used; and (4) there would be no independent agency to oversee the government's program. Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining*, 48 B.C. L. REV. 609, 649-62 (2007).

177. It has been stated that evaluating the NSA call database in other countries is important because "it could undermine transatlantic cooperation in the fight against terrorism. Some European laws forbid the transfer of public security and law enforcement data to countries without adequate privacy protection." Posting by Francesca Bignami to Concurring Opinions, http://www.concurringopinions.com/archives/2006/05/the_nsa_phone_c.html (May 29, 2006, 03:51 EST).

178. The purpose of this part is to use the facts from the NSA call database in the United States as the foundation for the international analysis in Canada, the United Kingdom, and Australia. Thus, all the facts from the background found in Part I of this Note are assumed.

179. Privacy International, About Privacy International, http://www.privacyinternational.org (last visited Feb. 12, 2007) (stating that "Privacy International . . . is a human rights group formed in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations").

180. Privacy International, Leading Surveillance Societies in the EU and the World, Feb. 11, 2006, http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-545269.

181. *Id.*

that other countries strike between national security and privacy rights.[182]

A. Canada

1. Obtaining Phone Records.[183] In 2001, Canada enacted the Personal Information Protection and Electronic Documents Act (PIPEDA)[184] to protect an individual's privacy interests and to prevent "secret information gathering practices."[185] Specifically, § 7(3) of PIPEDA prevents personal information,[186] such as phone records, from being disclosed by a telecommunication provider without consent, subpoena, warrant, or court order.[187] However, the national security clause of PIPEDA allows disclosure to the government without the individual's consent when the government has "identified its [1] *lawful authority* to obtain the information *and* . . . (i) it *suspects* that the information [2] relates to *national security*."[188]

PIPEDA does not define "lawful authority" or what authority is necessary for "obtaining and possessing the information."[189] However, an Ontario court has recently attempted to interpret "lawful authority."[190] In that case, the police requested an internet subscriber's information from Bell Canada under PIPEDA,[191] citing

182. The international discussion does not address the possibly higher level of privacy imposed by the various states or provinces' statutes or common-law privacy within each country. Moreover, this part does not discuss possible defenses available to each country's government.

183. Currently, Canada has proposed federal legislation called The Modernization of Investigative Techniques Act (MITA). Canadian Security, Do You Know Where Your Data is Stored?, http://www.canadiansecuritymag.com/index.php?option=com_content&task=view&id=245&Itemid=5 (last visited Feb. 14, 2007). MITA "will permit law enforcement to request any information about a subscriber from a communications provider, *without* requiring judicial authorization." *Id.* (emphasis added).

184. Personal Information Protection and Electronic Documents Act, 2000 S.C., ch.5 (Can.) [hereinafter PIPEDA].

185. Arthur J. Cockfield, *Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance*, 29 QUEEN'S L.J. 364, 405 (2003).

186. Section 2 of PIPEDA defines "personal information" as "information about an identifiable individual." PIPEDA § 2.

187. Jonathon Gatehouse, *You are Exposed*, MACLEANS.CA, Nov. 21, 2005, http://www.macleans.ca/canada/national/article.jsp?content=20051121_115779_115779.

188. PIPEDA § 7(3)(cl.1) (emphasis added).

189. *In re* S.C., [2006] O.J. No. 3754 (Ont.).

190. *Id.*

191. *See id.*

an ongoing investigation as its authority for the information.[192] Based on this authority, Bell Canada provided the information without a warrant.[193] The court held that an ongoing criminal investigation does not constitute "lawful authority," and that a warrant was necessary to obtain the subscriber information under PIPEDA because the individual held a reasonable expectation of privacy in it.[194]

This case indicates that the government must have more than a mere suspicion of wrongdoing before it is acting with the requisite "lawful authority." Here, it is doubtful that the government has met the "lawful authority" burden, as it will not know until after the records are mined or searched whether they are relevant to any wrongdoing.[195] If collection was allowed, it would be based on nothing more than a "fishing expedition." While it is true that call records, unlike the subscriber information, do not implicate the same expectation of privacy, it is arguable that a person does have at least some expectation of privacy in records disclosed to third parties, as will be discussed.

Besides the lawful authority requirement, the national security clause also requires the government to "*suspect*[] that the information [obtained] *relates* to *national security*."[196] National security is difficult to define and the definition is not found within PIPEDA;[197] however, a Supreme Court of Canada decision[198] in 2002 may be read "as . . . [signaling] a limited role for the courts in policing the exercise of executive branch" in determining what constitutes national security.[199] Notwithstanding this possible limited role by courts, it is unlikely the government had enough suspicion as required by the national security clause to justify the acquisition of phone records.

Any suspicion likely requires some investigation by the government to determine whether the information relates to national

192. *See id.*

193. *See id.*

194. *Id.*

195. *See* Letter from Electronic Frontier to Lawful Access Consultation (Dec. 17, 2002) (available at http://www.efc.ca/pages/surveillance/lawful.doc).

196. PIPEDA, 2000 S.C., ch.5 § 7(3)(cl.1) (emphasis added).

197. Craig Forcese, *Through a Glass Darkly: The Role and Review of "National Security" Concepts in Canadian Law*, 43 ALBERTA L. REV. 963 (2006) (stating that "national security is not defined in any of the other privacy-limiting statutes").

198. Suresh v. Canada (Minister of Citizenship and Immigration), [2002] 1 S.C.R. 3.

199. Forcese, *supra* note 197.

security.[200] This is necessary to ensure that a person's privacy is protected and that the government is not arbitrarily obtaining the information without some justification. Further, this suspicion requirement also protects a person from the stigma attached to being mistakenly labeled a national security suspect. Thus, because the request for call records would not be predicated on any suspicion,[201] there would be no nexus to national security justifying the request.

In addition to PIPEDA, the Canadian Privacy Act (CPA) requires that the government minimize the collection of personal information[202] and have a demonstrable need for it.[203] CPA is similar to PIPEDA, except that it is concerned with government entities as opposed to private ones. Section 4 of the CPA provides that personal information should not be collected except when it relates to a government program;[204] § 5(1), in contrast, requires that information be collected, if possible, directly from the person.[205] Thus, for similar reasons discussed under PIPEDA, and the fact that the data collection would not be minimized, the government could not feasibly collect call records from the phone providers.

2. Datamining the Call Records. The next issue is whether datamining the call records would violate § 8 of the Canadian Charter of Rights and Freedoms (the Charter), which states that a person has a right to be protected against "unreasonable search and seizure."[206] The analysis under § 8, like that under the Fourth Amendment, is divided into two prongs: first, does the person have a reasonable

200. *In Re* Ontario Power Generation Inc. and Society of Energy Prof'ls, [2004] C.L.A.S.J. 9606 para. 28 (Ont.) (holding that the information required by the Canadian Nuclear Safety Commission was "predicated upon the need to do so for national security reasons").

201. *See* background discussion *supra* Part I.

202. Section 2 defines personal information as "information about an identifiable individual." Privacy Act, R.S.C., ch. P 21 (1985) (Can.) [hereinafter Canadian Privacy Act].

203. News Release, Office of the Privacy Commissioner of Canada, Privacy Commissioner releases finding on video surveillance by RCMP in Kelowna (Oct. 4, 2001) (available at http://www.privcom.gc.ca/media/nr-c/02_05_b_011004_e.asp).

204. Canadian Privacy Act § 4.

205. *Id.* Section 8(2) provides numerous exceptions for when an agency can disclose (not collect) personal information to another government agency. This section focuses on whether the Canadian government could collect the personal information in the first instance from the telecommunications provider and not whether it could obtain the data from some other government agency. *See id.* § 8(2).

206. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, para. 8, being Sched. B to the Canada Act 1982, ch. 11 (U.K.).

expectation of privacy in his or her phone records;[207] and second, is datamining those phone records reasonable.[208]

a. Reasonable Expectation of Privacy. The first prong potentially contains a number of factors that are relevant in determining whether a person has a reasonable expectation of privacy in his or her phone records.[209] First, it is relevant whether the information was disclosed to a third-party.[210] Unlike American law, where the Supreme Court has held that a person does not have a reasonable expectation of privacy in any records disclosed to a third-party,[211] the "Charter jurisprudence acknowledges the persistence of constitutionally protected interests in information disclosed to third parties."[212] For example, a person in Canada has a reasonable expectation of privacy in information provided to a physician and information provided to a third-party regarding a sexual assault.[213] Thus, in contrast with American law, under Canadian law, a privacy expectation is not automatically lost when information is disclosed to a third-party custodian.[214]

A second factor is the place where the search occurred and the technology used in the search.[215] The Canadian Supreme Court has suggested that government searching of third-party records is not as constitutionally protected as the searching of a person's home.[216] This may be true, but it does not necessarily follow that individuals have no expectation of privacy in their records.[217] Moreover, the place of the search is not constitutionally determinative because § 8 "protects people, not places."[218] As for the technology used in the search, the ability of datamining programs to search vast quantities of data in minutes is constitutionally problematic.

---

207. *See* Wayne N. Renke, *Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy*, 43 ALBERTA L. REV. 779, 800 (2006).

208. *See id* at 810.

209. *Id.* at 800-01.

210. *Id.* at 803.

211. United States v. Miller, 425 U.S. 435, 444-45 (1976); Smith v. Maryland, 442 U.S. 735, 742 (1979).

212. Renke, *supra* note 207, at 803.

213. *Id.*

214. *See id.*

215. *See id.* at 806-07, 809.

216. *Id.* at 806 (citing R v. Plant, [1993] S.C.R. 281, 295).

217. *Id.* at 807.

218. *Id.*

A third factor in the reasonable privacy expectation calculus is the individual's conduct.[219] This factor requires determining the context[220] or reason for disclosure by the individual. After a call is made, phone providers automatically create call records.[221] However, "[m]ost Canadians consider their call records privileged information"[222] and thus do not believe they are making any public disclosure when a call is placed. Accordingly, the acquisition of call records by the government from the phone providers is likely an involuntary disclosure.

Fourth, the nature of the information may be another important factor.[223] Generally, the "greater the relevance of the information to the 'biographical core' of the individual, to the 'intimate details' of the individual's life . . . the stronger the expectation of privacy."[224] Although call records do not appear to identify biographical core information, the Canadian Criminal Code "establishes a procedure for the issuance of a warrant to install a device and record this information."[225] Thus, the Criminal Code provision is evidence that call records have some constitutional value.

The final factor is the relationship between the custodian (government or phone provider) and the individual.[226] Both PIPEDA and the CPA statutorily require that the custodian protect private information such as call records.[227] Based on these statutes, it is likely that a person would reasonably rely on them to protect his privacy expectations.

b. Is Datamining the Call Records Reasonable? In analyzing the second prong, whether datamining is reasonable, there are five potentially relevant factors to consider. The first is the purpose of the datamining.[228] Here, the purpose of the mining would be to prevent terrorist acts, which is unquantifiably important. Datamining without any purpose other than to protect the monolithic category of "national security" should not suffice. Response to terrorism

219. *Id.* at 801.
220. *Id.*
221. Diamond & Cauley, *supra* note 5.
222. Gatehouse, *supra* note 187.
223. Renke, *supra* note 207, at 803-04.
224. *Id.* at 803; R.S.C., ch. C-46, § 492.2 (1985).
225. Renke, *supra* note 207, at 804.
226. *See id.* at 804-06.
227. *Id.* at 804-05.
228. *See id.* at 811-12.

sometimes means that the government must move quickly, such as in an emergency,[229] but when an emergency exists, the constitutional protections of the Charter should not be sacrificed.

The second factor looks at whether the datamining is effective.[230] The individuals in the call database were not selected based on an investigation. Thus, many false positives are likely to result, especially considering the size of the database, which involves millions of people. Moreover, the patterns that emerge from the mining depend on the suspect maintaining a similar history, but "as adversaries change strategy, their patterns of past behavior fail to provide clues to future activities."[231] Finally, the patterns that do emerge may be questionable for the simple reason that the dataset supporting the pattern is not large enough (lack of suspects) to make any accurate statistical predictions.[232]

A third factor in the reasonableness calculus is the intrusiveness[233] of mining the data. The Canadian Supreme Court has stated that the scope of invasion can make a search unreasonable, especially when the people searched are not under any investigation.[234] The American call database, however, would likely involve millions of targets and a person's call records being repeatedly searched.

In addition to the purpose, effectiveness, and intrusiveness of datamining, another factor to consider is whether there is any oversight of the datamining.[235] Oversight aids in eliminating any potential distrust between the people searched and the government.[236] As discussed previously, the NSA call database lacks any appearance of oversight, as the program was created secretly and without the input from the people's representatives.[237] Thus, Canadians would probably distrust datamining more than if they were informed about the data searching before it occurred. It could be argued that giving notice to people would completely destroy the national security

229. *See id.*

230. *Id.* at 816-17.

231. *Data mining*, WIKIPEDIA, http://en.wikipedia.org/wiki/Data_mining (last visited Feb. 14, 2007).

232. *Id.*

233. Renke, *supra* note 207, at 813-14.

234. *Id.* at 813 (citing R v. Thompson, [1990] S.C.R. 1111, 1143-44).

235. *Id.* at 820.

236. *See id*.

237. Page, *NSA Secret Database*, *supra* note 2.

purpose, as possible terrorists would alter their plans. However, this argument ignores that there are alternative ways to prevent tipping off the potential terrorists, but at the same time providing the requisite notice. For instance, the government could limit the call records to known investigations of terrorist suspects or call records for which the government has a warrant.

The final consideration in determining the reasonableness of the search is the potential misuse of the data.[238] It is possible that one agency could make the call database available to other agencies,[239] thereby allowing them to obtain call records about a person without any investigation or probable cause. Moreover, hackers could penetrate the government's security and consequently share that information almost instantly with the world.[240] The size of the database makes these threats even more serious.

B. United Kingdom

1. Obtaining Phone Records. In December of 2001, the British Parliament approved the Anti-Terrorism, Crime and Security Act (ATCSA).[241] ATCSA allows the government to request that communication providers retain their data[242] for national security purposes or for preventing crimes that relate to national security.[243] In addition to ATCSA, the United Kingdom has also enacted the Regulation of Investigatory Powers Act (RIPA), which controls "the acquisition and disclosure of data relating to communications."[244] Specifically, under § 22(2) of RIPA, a number of government groups can access personal information outside of national security for such things as the collection of taxes.[245]

---

238. Renke, *supra* note 207, at 818-19.

239. *See id.* at 819.

240. *See id.* at 819-20.

241. Anti-Terrorism, Crime and Security Act, 2001 (U.K.) [hereinafter ATCSA]; *see also* PRIVACY INT'L, PRIVACY AND HUMAN RIGHTS 2005, at 661, 726 (2005), *available at* http://www.privacyinternational.org/survey/phr2005/PHR2005swed-ven.pdf [hereinafter PRIVACY AND HUMAN RIGHTS].

242. Whether the retention is illegal under Article 8 of the European Convention on Human Rights (ECHR) is beyond the scope of this Note. *See* Hosein et al., *supra* note 142 (arguing that data retention would be illegal because it would interfere with Article 8 of ECHR—"the right to respect for his or her private life"—by accumulating a large amount of private data).

243. ATCSA, pt. 11; PRIVACY AND HUMAN RIGHTS, *supra* note 241, at 726.

244. Regulation of Investigatory Powers Act, 2000 (U.K.) [hereinafter RIPA].

245. Ben Emmerson, Q.C. & Helen Mountfield, Counsel to the Info. Comm'r, *Anti-Terrorism, Crime And Security Act 2001 Retention And Disclosure Of Communications Data*

As a result of both ATCSA and RIPA, data can be retained for national security purposes, but can be accessed by a wide variety of public groups for "purposes . . . which extend substantially beyond issues concerning national security."[246] In fact, the Home Office[247] stated in 2002 that under RIPA more than "1,000 different government departments including local authorities, health, environmental, trade departments and many other public authorities" had access to the communications data.[248]

Through these acts, the British government has already created something like the call database. The telecommunication providers can be required to retain the call records and many governmental units have access to them. Thus, the acquisition of call records by the government would likely be legal under British law.

2. Datamining the Call Records. It has been claimed by some commentators that even though the United Kingdom's anti-terrorism legislation does not address datamining, it "is already widely used in the United Kingdom to combat terrorism."[249] Further, it would seem incongruent to have broad laws enabling the retention of data, but not allowing the mining of that data. Thus, a final question that needs to be addressed is whether the U.K. government could permissibly search the call records.

Like many other European Countries, the United Kingdom has adopted the European Convention on Human Rights (ECHR).[250]

Summary Of Counsels' Advice, para. 4, http://www.privacyinternational.org/countries/uk/surveillance/ic-terror-opinion.htm [hereinafter Counsels' Advice] (stating that the RIPA "permits a range of public authorities to obtain access to such communications data for a wide variety of public interest purposes . . . which extend substantially beyond issues concerning national security"). Section 22(2) of the RIPA lists eight possible reasons for the government to obtain communication data. RIPA § 22(2).

246. Counsels' Advice, *supra* note 245.

247. The Home Office is "responsible for keeping the UK safe from any threat to . . . national security . . . [by working] with the police and security agencies." Home Office, Security, http://www.homeoffice.gov.uk/security/ (last visited Feb. 4, 2007).

248. PRIVACY AND HUMAN RIGHTS, *supra* note 241, at 726.

249. John Yoo, *Catching Terrorists: The British System versus the U.S. System*, AM. INST. FOR PUB. POL'Y RES., Sept. 18, 2006, http://www.aei.org/publications/filter.all,pubID.24903/pub_detail.asp; *see generally* Kendra Gilbert, *Gregg: Fight Terrorism like the British*, THE UNION LEADER (N.H.), Sept. 15, 2006, at A7 (stating that some believe "the U.S. government [should] emulate Britain's *more lenient restrictions on data mining*") (emphasis added).

250. *See generally* DANIEL C. PREFONTAINE, THE INT'L CTR. FOR CRIMINAL LAW REFORM AND CRIMINAL JUSTICE POLICY, IMPLEMENTING INTERNATIONAL STANDARDS IN SEARCH AND SEIZURE: STRIKING THE BALANCE BETWEEN ENFORCING THE LAW AND RESPECTING THE RIGHTS OF THE INDIVIDUAL 5 (2001), *available at* http://www.icclr.law.ubc.ca/Publications/

Under Article 8(1), "[e]veryone has the right to respect for his private . . . .life."[251] This has been read as the right to be free from government interference except when the government's interference is "in accordance with the law and is necessary in a democratic society in the interests of national security."[252]

The first question is whether the search of call records amounts to an interference requiring the government to justify its actions. Article 8's reference to private life means that a person has a right to seek and form relationships with other individuals.[253] Searching call records could chill the use of phones to communicate with others and accordingly would interfere with the private life protected by Article 8.[254] It could be argued that no interference exists because the data searched is limited to non-content communications data.[255] However, this argument ignores that the "European Court of Human Rights has repeatedly found the recording of numbers [dialed] from conventional telephones to constitute an interference with private life." [256] Moreover, after considering the scope of the call database, the interference is significant, even conceding that only non-content information is being searched.

Although there may be interference, the government may not have violated Article 8 if the interference is "in accordance with the law . . . and necessary in a democratic society."[257] In 2000, the European Commission on Human Rights (the precursor to the European Court of Human Rights), in *Khan v. United Kingdom*,[258] discussed the meaning of "in accordance with law." In *Khan*, the court stated:

Reports/International_Standards.pdf. In 1998, the U.K. Parliament adopted The Human Rights Act, which contains three points regarding the ECHR: (1) the government cannot violate Convention rights unless, through an Act of Parliament, it had no choice; (2) U.K. legislation should be interpreted to fit within the ECHR; (3) individuals can seek a remedy from a U.K. court instead of using the European Court of Human Rights. Dep't for Constitutional Affairs, General Information on the Human Rights Act 1998, http://www.dca.gov.uk/peoples-rights/human-rights/faqs.htm (last visited Jan. 15, 2007).

251. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8(1), Nov. 4, 1950, Europ. T.S. No. 5 [hereinafter ECHR].

252. *Id.* art. 8(2).

253. *See* Hosein et al., *supra* note 142.

254. *See id.*

255. *See id.*

256. *See id.*

257. ECHR, *supra* note 251, art. 8(2).

258. App. No. 35394/97, 31 Eur. H.R. Rep. 45 (2001) (Commission Report).

> [T]he phrase "in accordance with the law" not only requires *compliance with domestic law* but relates to the quality of that law . . . the law must be sufficiently clear in its terms to give individuals an *adequate indication* as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures.[259]

Khan requires the existence of a domestic law that sanctions the interference and a law that allows individuals to foresee when the government can interfere in their private lives.[260] This foreseeability function permits individuals to adjust or alter their conduct to avoid the possible interference.[261] Without this notice, for example, an individual may be penalized for previously legal conduct. Even if the United Kingdom enacted laws that authorized datamining to prevent terrorism, the laws would still have to be sufficiently public to put the citizens on notice, which did not happen based on the alleged facts from the NSA call database. Thus, the United Kingdom's action of datamining would likely not be "in accordance with the law."

Even though the government's datamining is not "in accordance with the law," it is still valuable to discuss whether the datamining "is necessary in a democratic society." The European Court on Human Rights has interpreted this phrase to mean that the interference has to be *proportionate* (or no more than necessary) to a "legitimate aim pursued" and must "correspond to a pressing social need."[262]

In considering how the call database would fare under U.K. law, the proportionality requirement is not met because the United Kingdom has no mechanisms in place to limit the interference. First, the government did not restrict its datamining to the call records of suspected terrorists. Instead, the government mined the records of individuals merely because they made a domestic phone call. Second, if the government does not destroy the call records after mining, then it would be continually interfering with a person's life[263] because the

---

259. *Id.* at para. 26 (emphasis added); *see generally* Alisdair A. Gillespie, *The Legal Use of Participating Informers*, WEB J. OF CURRENT LEGAL ISSUES (2000), http://webjcli.ncl.ac.uk/2000/issue5/gillespie5.html.

260. *Khan*, 31 Eur. H.R. Rep. 45, para. 26.

261. Hosein et al., *supra* note 142.

262. *Id. See also, e.g.*, Case C-441/02, Comm'n v. Germany, 2006 E.C.R. I-03449 para. 109 (The European Court of Justice stated that for something to be "necessary in a democratic society," it must be "justified by a pressing social need and, in particular, proportionate to the legitimate aim pursued."); Case C-540/03, Parliament v. Council, 2005 E.C.R. I-8667.

263. *In Re* S. v. Chief Constable of South Yorkshire, [2004] UKHL 39 ("The general tenor of the jurisprudence of the European Court of Human Rights (the Court of Human Rights) and European Commission of Human Rights (the Commission) is that the retention, keeping or

retention of data would allow any government agency to perform surveillance at will.[264] Finally, one person's records may be searched multiple times without any oversight procedures to ensure the search is limited. Accordingly, it is unlikely that datamining by the U.K. government "is necessary in a democratic society."

In addition to the ECHR, there is a British domestic law that protects data processing called the Data Protection Act.[265] This Act applies to personal data[266] processing done by government and private organizations.[267] The Act contains eight principles illustrating how personal data should be processed.[268] The Act, however, is not considered effective because "[t]here are many problems with *enforcing rules* on access to information, especially relating to computer technologies."[269] Moreover, a recent Court of Appeals decision has narrowed the meaning of "personal information" and thus restricted the possible privacy protections under the Act.[270] It is therefore likely that the ECHR rather than the domestic law provides more protection against unlawful datamining.

---

storage of private information by state institutions is an interference with art. 8(1) rights."); *see also* Hosein et al., *supra* note 142.

264. *See id.* (stating "that citizens should have notice of the circumstances in which the State may conduct surveillance, so that they can regulate their behaviour to avoid unwanted intrusions").

265. Data Protection Act, 1998 (U.K.) [hereinafter DPA]; PRIVACY INT'L, UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND 2003, *available at* http://www.privacyinternational.org/survey/phr2003/countries/unitedkingdom.htm [hereinafter UNITED KINGDOM]; Spy Blog, RFID Data Protection Guidance from the Information Commissioner, http://p10.hostingprod.com/@spyblog.org.uk/blog/2006/09/rfid_data_protection_guidance.html (Sept. 28, 2006, 11:57 AM) (stating that "[t]he Data Protection Act 1998 concerns the processing of personal data").

266. DPA pt. 1, § 1 (defining "personal data," in part, as "data which relate to a living individual who can be identified . . . from those data").

267. UNITED KINGDOM, *supra* note 265.

268. *See* Margaret Smith, *The Privacy of Personal Information and Electronic Commerce—Recent Developments*, GOV'T OF CAN. PUBLICATIONS, May 31, 2000, *available at* http://dsp-psd.communication.gc.ca/Pilot/LoPBdP/BP/prb0005-e.htm.

269. UNITED KINGDOM, *supra* note 265 (emphasis added); Anne Lenoir, *Privacy and Data Protection Act 2007*, BBC ACTION NETWORK, Dec. 19, 2006, http://www.bbc.co.uk/dna/actionnetwork/A4446038 (arguing the Data Protection Act of 1998 does not protect the right of privacy).

270. *Data protection case goes to the House of Lords*, OUT-LAW NEWS, June 16, 2005, http://www.out-law.com/page-5820; Jason Lysandrides, *UK Government Given Formal Warning by Commission*, LAWDIT READING ROOM, http://www.lawdit.co.uk/reading_room/room/view_article.asp?name=../articles/Privacy%20developments%20-%20draftv2.htm (last visited Jan. 15, 2007) (stating the European Commission issued a formal warning to the U.K. government because "the narrow interpretation given . . . of personal data . . . [does] not adequately reflect the broader intention of the [European Union]").

C. Australia

1. Obtaining Phone Records. In 1997, Australia enacted the Telecommunications Act, which "contains a number of provisions dealing with the privacy of personal information held by" providers.[271] Under Part 13 of that Act, it is presumed that a consumer's phone records are confidential unless an exception applies.[272] One such exception allows disclosure to an Australian Security Intelligence Organization (ASIO) agent when it is authorized "in writing by the Director-General of Security" (DGS) and the disclosure relates to the ASIO functions.[273] The DGS could potentially authorize the telecommunication providers to disclose millions of call records. However, it is unlikely that the DGS would make such certification equivalent to the American database, because it is doubtful that such a broad request would relate to ASIO functions.[274]

Even without the ASIO exception, it may still be possible for the Australian government to obtain the call records through the Telecommunications Act by leveraging records already obtained through other agencies.[275] The Act permits disclosure to the government for the "enforcement of the criminal law."[276] In 2001, approximately 750,000 call records were released to governmental units,[277] and in 1999-2000 almost one million disclosures of records

271. The Office of the Privacy Commissioner, http://www.privacy.gov.au/act/telecom/index.html (last visited Feb. 13, 2007).

272. PRIVACY INT'L, COMMONWEALTH OF AUSTRALIA (2003), http://www.privacyinternational.org/survey/phr2003/countries/australia.htm (stating that "[t]he Telecommunications Act 1997 contains a detailed list of 'exceptions' from a basic presumption of confidentiality of customer records"). Part 13 § 276(1)(a) of the 1997 Telecommunications Act prohibits disclosure of information that relates to the communication substance unless an exception applies. Telecommunications Act, 1997, pt. 13, § 276(1)(a) (Austl.). Because call records contain data that relates to the substance of the communication such as where the call was made, those records would likely qualify as information that could not be disclosed without an exception.

273. Telecommunications Act, pt. 13, § 283.

274. *But see infra* note 277 (discussing that a substantial number of call records have been disclosed to the ASIO).

275. This analysis assumes that the other agencies have kept a repository or database of call records once obtained from the telecommunication provider and have not erased these records.

276. Telecommunications Act, pt. 13, § 282.

277. Velcro, *supra* note 22; *see Protection of Communications: Telecommunications Act 1997 (C'th)*, ELECTRONIC FRONTIERS AUSTL., Oct. 12, 2006, http://www.efa.org.au/Issues/Privacy/ta.html (stating that "[t]he Australian Communications Authority has confirmed that telecommunications companies . . . [disclosed] information to law-enforcement and other government agencies 998,548 times in 1999-2000. . . . The extraordinary access to phone records *does not include* information given to the Australian Security Intelligence Organisation, *which is believed to be substantial* and which the agency is not obliged to disclose. The information

were made under the Act.[278] Moreover, any agency that gives call records or personal information to an intelligence agency would be exempt from the requirements of the Federal Privacy Act,[279] which limits the collection of personal information by the government.[280] Thus, the police and other agencies could obtain the call records and then transfer those records to an intelligence agency in a manner similar to the FBI acquiring and transferring call records to the NSA.

In addition to the Telecommunications Act of 1997, the amended 2001 Federal Privacy Act limits the government's ability to acquire call records.[281] This Act includes National Privacy Principles (NPP) [282] and Information Privacy Principles (IPP),[283] but unlike the NPPs, which apply to private organizations, the IPPs apply to government agencies.[284] Specifically, NPP 2 states that a telecommunication

---

revealed included telephone accounts, numbers dialled, the time calls were made and their duration, and use of the Internet. These disclosures were made at a rate of more than 19,000 a week, or nearly 4000 on any working day.") (emphasis added).

278. *Inquiry into The Law Enforcement Implications of New Technology*, ELECTRONIC FRONTIERS AUSTL., Apr. 19, 2001, http://www.efa.org.au/Publish/ncasub.html.

279. Part 2, § 7(1) of the Privacy Act states that a "record that has originated with, or has been received from . . . an intelligence agency" is exempt from the Privacy Act. Privacy Act, 1988, as amended 2006, pt. 2, § 7(1) (Austl.); *see* Roger Clark, *The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines*, THE AUSTL. NAT'L U., June 25, 1989, *available at* http://www.anu.edu.au/people/Roger.Clarke/DV/PActOECD.html (stating that § 7(1) has "the effect that any record whatsoever can be permanently removed from the individual's sight by passing the data to an intelligence agency for its consideration and return. Any material that an agency wishes to keep from a data subject can therefore be protected.").

280. Matthew Kohel, Note, *The Privacy Amendment (Private Sector) Bill 2000: The Australian Government's Substandard Attempt to Allay Privacy Concerns and Regulate Internet Privacy in the Private Sector*, 27 BROOKLYN J. INT'L L. 703, 703-04 (2002) (stating that "[t]he Privacy Act was Australia's attempt to regulate how personal information is collected, transferred and disposed of in the public sector").

281. It is true that the Telecommunications Act of 1997 and the Amended Privacy Act of 2001 would seem to overlap, however, the "[c]overage of the National Privacy Principles in the Privacy legislation is broader than Part 13 of the Telecommunications Act." Holly Raiche, *Telecommunications Privacy—The Interaction of the Privacy and Telecommunications Regulatory Systems*, THE NEW AUSTL. PRIVACY LANDSCAPE CONTINUING LEGAL EDUC. SEMINAR (Mar. 14, 2001) *available at* http://www.worldlii.org/int/other/PrivLRes/2001/4.html.

282. Office of Legislative Drafting, Extracted from the Privacy Act 1988, http://www.privacy.gov.au/publications/npps01.pdf (last visited June 14, 2007) [hereinafter National Privacy Principles].

283. The Information Privacy Principles are a part of the 1988 Privacy Act. Privacy Act, 1988 (Austl.) [hereinafter Information Privacy Principles].

284. *See* The Office of the Privacy Commissioner, Federal Privacy Law, http://www.privacy.gov.au/act/index.html (last visited Apr. 11, 2007) (stating that in Australia, "[t]he Federal Privacy Act contains eleven Information Privacy Principles (IPPs) which apply to Commonwealth and ACT government agencies. It also has ten National Privacy Principles (NPPs) which apply to parts of the private sector and all health service providers."). Therefore,

provider "must not . . . disclose personal information[285] about an individual for a purpose (the secondary purpose) other than the primary purpose of collection" unless an exception applies.[286]

The primary purpose of the collection of the call records by the telecommunication providers will probably be for billing even though other purposes may be listed in the standard phone contract. It is highly unlikely that phone providers collect call records primarily for national security. Thus, the phone providers could not disclose personal information unless it was for billing purposes.

Although NPP 2 prohibits disclosure of call records, it still allows disclosure for a secondary purpose if an exception applies. It is unlikely that the phone providers could have a secondary purpose because "there must be a strong[] connection between the . . . disclosure and the primary purpose for collection."[287] A national security purpose would not have a strong connection to billing and therefore not qualify as a secondary purpose.

Even assuming that the phone providers had an arguable secondary purpose, none of the exceptions list in NPP 2.1(a)-(h)

---

because the Federal Privacy Act "does not regulate state or territory agencies, except for the ACT," any analysis of the call database would have to be done under each state's privacy laws, which is beyond the scope of this Note. Office of Privacy Commissioner, State & Territory Privacy Laws, http://www.privacy.gov.au/privacy_rights/laws/index.html (last visited Apr. 10, 2007).

285. Personal information is defined as "an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or *can reasonably be ascertained, from the information* or opinion." Privacy Act, 1988, as amended 2006, pt. 2, §6(1) (Austl.). Thus, call records would likely fit within the definition as a person's identity can be reasonably ascertained from person's phone number by matching that number to a name in the phone book. *See* Sarah Harrison, *The Privacy Amendments—What Do They Mean for General Insurance Claims?*, 2002 INS. L.J. (Austl.) 13 n.18 (July 26, 2002) (defining personal information as "a person's name, address, *phone number*, email address, birth date, marital information etc.") (emphasis added).

286. National Privacy Principles Act, *supra* note 282, § 2.1. The exceptions are found under 2.1 and include (a) where "the secondary purpose [of disclosure] is related to the primary purpose of collection and . . . the individual would reasonably expect the organization to . . . disclose the information for the secondary purpose"; (b) consent by a person; (c) the person's non-sensitive information will be used for direct marketing and five other conditions are met; (d) the person's health information is required for research related to public safety and three other conditions are met; (e) disclosure is necessary to protect an imminent threat to a person's safety, health, or life or "a serious threat to public health or public safety"; (ee) genetic information obtain through providing health service and three other conditions are met; (f) organization believes that unlawful activity is occurring and discloses the personal information for an investigation; (g) authorized by law; (h) disclosure is necessary for an enforcement body such as law enforcement or public revenue protection. *Id.* § 2.1(a)-(h).

287. Office of the Privacy Comm'r, Guidelines to the National Privacy Principles, Sept. 2001, http://www.privacy.gov.au/publications/nppgl_01.html [hereinafter Guidelines].

likely applies.[288] The only exceptions likely to apply are that the disclosure is necessary to prevent an imminent or serious threat[289] or is necessary for an enforcement body.[290] The threat exception is not applicable because most, if not all, the records were collected to prevent possible future threats, and this exception allows disclosure in emergency situations only.[291] Under the enforcement body exception, disclosure is permitted to prevent or investigate a criminal offense,[292] which is "an act or practice that is prohibited by criminal law at Commonwealth or State and Territory level."[293] Thus, disclosure of call records would not be permitted because there is no criminal act.

Notwithstanding the limitation imposed on the telecommunication providers through the NPPs, the government could still not acquire the call records based on the IPPs. Under IPP 1, the government can only collect personal information lawfully, and the collection has to be related to the government's purpose.[294] Moreover, IPP 3 states that when the government requests personal information, the information must be relevant to the agency's reason for collecting it.[295] If the government collected numerous call records, it would violate IPP1 for two reasons. First, it would be acting without a warrant and therefore unlawfully. Second, any collected call records would not have the necessary connection to terrorism and therefore fail to serve the government's terrorist prevention purpose.

2. Datamining the Call Records. Australia's federal constitution does not include provisions relating to privacy.[296] In fact,

---

288. It is unlikely a person consents to datamining for national security purposes through phone contracts and the direct marketing, unlawful activity, authorized by law, health, and genetic exceptions are not applicable.

289. National Privacy Principles Act, *supra* note 282, § 2.1(e).

290. *Id.* § 2.1(h)(i)-(v).

291. Guidelines, *supra* note 287.

292. National Privacy Principles Act, *supra* note 282, § 2.1(h)(i).

293. *INFORMATION SHEET 7—2001 Unlawful Activity and Law Enforcement*, OFFICE OF THE PRIVACY COMM'R (Dec. 2001), *available at* http://www.privacy.gov.au/publications/IS7_01.doc.

294. *Plain English Guidelines to Information Privacy: Principles 1- 3*, OFFICE OF THE PRIVACY COMM'R, 2 (1994), *available at* http://www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.word_file.p6_4_14.4.doc.

295. *Id.* at 4.

296. LEGAL & CONSTITUTIONAL REFERENCES COMM., THE REAL BIG BROTHER: INQUIRY INTO THE PRIVACY ACT 1988, at 10 (2005) *available at* http://www.aph.gov.au/senate/committee/legcon_ctte/privacy/report/report.pdf
(stating that "[t]he Australian Constitution does not expressly protect privacy").

Australia currently does not have a bill of rights.[297] Australians must therefore turn to other sources of law, such as international agreements[298] or domestic privacy statutes, for protection against interference with their private life.

Australia ratified the International Covenant on Civil and Political Rights (ICCPR) in 1980.[299] Article 17 of ICCPR provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy . . . [and] [e]veryone has the right to the protection of the law against such interference."[300] Moreover, "any [arbitrary] interference with privacy must be *proportional* to the end sought and be *necessary* in the circumstances of any given case."[301]

Based in part on the ICCPR, the Australian government, in 1980, adopted a domestic Federal Privacy Act, discussed above, to protect against unlawful or arbitrary interference with privacy.[302] In particular, IPP 9 states that personal information can only be *used* by an agency "for a purpose to which the information is relevant."[303]

---

297. James Allan & Grant Huscroft, *Constitutional Rights Coming Home to Roost? Rights Internationalism in American Courts*, 43 SAN DIEGO L. REV. 1, 16 (2006).

298. LEGAL & CONSTITUTIONAL REFERENCES COMM., *supra* note 296, at 8 (stating that "[t]here are several key sources of international law and standards relevant to privacy protection in Australia. In particular, the International Covenant on Civil and Political Rights (ICCPR) recognises the right to privacy in Article 17."); *See* George Williams, *Bali, Terrorism & Australia: The Rule of Law and Human Rights in Australia after Bali*, AUSTL. POL'Y ONLINE, Nov. 19, 2002, http://www.apo.org.au/webboard/results.chtml?filename_num=00172 (stating that "the absence of a domestic Bill of Rights means that Australians turn to international law");

299. International Covenant on Civil and Political Rights, Dec. 16, 1966, 999 U.N.T.S. 171.

300. *Id.* art. 17. In addition to the ICCPR, Australia also ratified the Universal Declaration of Human Rights (UDHR) in 1948. Universal Declaration of Human Rights, G.A. Res. 217A (III), U.N. Doc. A/810 (Dec. 10, 1948). The UDHR in Article 12 contains a similar provision as ICCPR's Article 17 providing that "[n]o one shall be subjected to arbitrary interference with his privacy . . . . Everyone has the right to the protection of the law against such interference." *Id.* art. 12.

301. Human Rights Comm., *Views of the Human Rights Committee under article 5, paragraph 4, of the Optional Protocol to the International Covenant on Civil and Political Rights*, Commc'n No. 488/1992, ¶ 8.3, U.N. Doc CCPR/C/50/D/488/1992 (Mar. 31, 1994).

302. Chris Cowper, *Successful Complaints to the Federal Privacy Commissioner*, BAKER & MCKENZIE CYBERSPACE L. & POL'Y CTR. FOR CONTINUING LEGAL EDUC., Dec. 4, 2003, http://www.privacy.gov.au/news/speeches/sp22_03.doc (stating that "the Privacy Act was . . . a response to Australia's commitment as a party to the International Covenant on Civil and Political Right to 'adopt such legislative measures as may be necessary to gives effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, home, family or correspondence'").

303. *Plain English Guidelines to Information Privacy: Principles 8-11*, OFFICE OF THE PRIVACY COMM'R 4 (1996), *available at* http://www.privacy.gov.au/publications/ipp8_11.doc (stating that use includes "any accessing by an agency of personal information" such as searching records).

Additionally, IPP 10.1 states that personal information obtained by an agency can only be *used* for a particular purpose unless one of the five exceptions applies.[304] Further, that purpose must be well defined, that is, the agency "must know exactly why it is obtaining the information."[305]

Both IPP 9 and 10 and Article 17 of ICCPR would be violated if the government mined the call records for national security reasons. First, millions of call records would belong to people who are not terrorist suspects, thereby violating the relevance requirement in IPP 9. Next, the purpose would not be sufficiently well-defined or specific to satisfy the requirements of IPP 10.1 because it would be so broad as to include almost all personal information. Moreover, none of the five exceptions in 10.1(a)-(e) likely apply to exempt the government from IPP 10.1.[306] Finally, mining millions of call records would violate Article 17 of ICCPR, as there are less intrusive means to protect national security.

CONCLUSION

In analyzing the NSA call database under U.S. law, the first legal question focused on whether the NSA could legally obtain call records from the telecommunication providers. If the NSA did not obtain a warrant, it violated FISA. Further, an examination of the Pen Register Statute revealed that although the government did not violate the statute, the government should be liable for circumventing it. Alternatively, the FBI could not obtain the call records and then transfer them to the NSA using a NSL. Finally, analysis of this first question concluded by finding that the phone providers violated the 1996 Telecommunications Act for voluntary disclosure of call records. However, the providers did not likely violate the 1986 Stored Communications Act because they transferred real time, as opposed to stored, records to the NSA.

The next question analyzed whether datamining the call records violated the Fourth Amendment's prohibition against unreasonable search and seizures. Both *Miller* and *Smith* likely dictate that a person has no reasonable expectation of privacy in their phone records voluntarily given to a third-party. However, it is conceivable that the Court could find that the searching technology employed by

304. Information Privacy Principles, *supra* note 283.

305. *Plain English Guidelines to Information Privacy: Principles 8-11*, *supra* note 303.

306. Information Privacy Principles, *supra* note 283.

the NSA requires such a privacy interest. Through opinion polls and lawsuits, society seems to be indicating that it would recognize such a privacy interest.

After analyzing the relevant two questions, the focus switched to defenses available to the government, such as the state secrets privilege and the President's authority (both express and inherent). Under the state secrets privilege, the government would likely prevail because there have been no public disclosures about the call database. As for the President's authority, he lacks both express authority under the AUMF and inherent authority to bypass FISA.

Finally, the call database was analyzed under Canadian, British, and Australian law, and it was determined that the call database program was likely illegal in all countries. Canada's PIPEDA and Privacy Act prevent the government from acquiring call records while § 8 of the Charter might prohibit mining of those records. The expansive national security legislation in the United Kingdom would seem to allow the collection of call records, but the ECHR would appear to prevent mining those records.

In Australia, the NPPs and IPPs would likely prevent the Australian government from acquiring call records unless it can obtain those records from another agency. Also, IPP 9 and 10 and Article 17 of the ICCPR would likely prohibit datamining, as its purpose would not be well-defined, and the call records themselves would not be relevant to the national security purpose.

In sum, this Note explores a wide range of legal issues connected to the privacy protections from government intrusions. In today's society, this is significantly important as new technology allows the government to use information in new and previously unimaginable ways. Thus, there needs to be protection to ensure that even when national security is at its pinnacle, privacy is not sacrificed without justification and never completely.