Vol. XLVII No. 3 BOSTON COLLEGE LAW REVIEW May 2006

BOSTON COLLEGE LAW REVIEW

Vol. XLVII No. 3 May 2006

DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL

David Alan Jordan

Vol. XLVII No. 3 BOSTON COLLEGE LAW REVIEW May 2006

DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL

David Alan Jordan*

Abstract: Information to, from, and about U.S. persons routinely comes into the possession of the National Security Agency (the "NSA") through the lawful warrantless surveillance of foreign persons abroad. The NSA's internal administrative guidelines allow such information to be disseminated to law enforcement if it evinces any criminal conduct on the part of the U.S. person. This information may therefore be used to initiate domestic criminal investigations against U.S. citizens and other protected persons despite the fact that no warrant authorized the initial surveillance. The NSA's guidelines contain no qualification as to the type of criminal offense that may be revealed, and no consideration of the individual's reasonable expectation of privacy. Using encrypted Internet telephony as an example, this Article proposes a change to the NSA's internal guidelines that would prevent dissemination of information gained through the frustration of the reasonable privacy expectations of protected persons unless exigent circumstances or serious threats to national security were presented.

* LL.M., New York University School of Law (2006); J.D., *cum laude*, Washington and Lee University School of Law (2003). Member of the District of Columbia Bar. This Article was written in conjunction with the 2005 Law and Security Colloquium at New York University School of Law. I would like to thank Noah Feldman, Stephen Holmes, Karen Greenberg, and the Center on Law and Security for putting together a truly remarkable colloquium. I am also grateful to Eyal Benvenisti, David S. Caudill, Simon Chesterman, Mark Drumbl, Michael Guttman, Eva Heinstein, Sheila Jordan, Frederic Kirgis, and Harold Wagner for their advice both during and after the drafting of this Article. I am solely responsible for any mistakes that remain.

> *The warrant clause of the Fourth Amendment is not dead language. . . . "It is not an inconvenience to be somehow 'weighed' against the claims of police efficiency. It is, or should be, an important working part of our machinery of government, operating as a matter of course to check the 'well-intentioned but mistakenly over-zealous executive officers' who are a part of any system of law enforcement."*
>
> —United States v. U.S. Dist. Court (Keith) (Powell, J.)[1]

Introduction

On December 16, 2005, the *New York Times* published a front-page story revealing the existence of a secret executive order issued by President George W. Bush in the months following the September 11, 2001 terrorist attacks on the United States.[2] According to the article, the executive order authorizes the National Security Agency (the "NSA") to conduct electronic surveillance on U.S. citizens and permanent residents inside the United States without first obtaining a warrant from the Foreign Intelligence Surveillance Court as mandated by the Foreign Intelligence Surveillance Act of 1978 ("FISA").[3] This appears to be a stark departure from the law governing domestic surveillance,[4] and it raises serious constitutional questions about the limits of presidential power in times following national emergencies.[5]

---

[1] 407 U.S. 297, 315–16 (1972) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).

[2] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1.

[3] *Id.*; *see* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 18 U.S.C. §§ 2511, 2518, 2519, 50 U.S.C. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871 (2000 & Supp. III 2003)) [hereinafter FISA], *amended by* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638.

[4] *See* U.S. Dep't of Defense, Reg. No. 5240.1-R, Procedures Governing the Activities of DOD Intelligence Components that Affect U.S. Persons, ¶ C5.1.2.1 (Dec. 1982) [hereinafter DoD Reg. No. 5240.1-R], *available at* http://www.dtic.mil/whs/directives/corres/pdf/52401r_1282/p52401r.pdf ("A [Department of Defense] intelligence component may conduct electronic surveillance within the United States for foreign intelligence and counterintelligence purposes *only* pursuant to an order by a judge of the court pursuant to the Foreign Intelligence Surveillance Act of 1978 . . . or pursuant to a certification of the Attorney General issued under the authority of Section 102(a) of the Act.") (citation omitted) (emphasis added).

[5] President Bush's secret executive order allowing warrantless domestic surveillance of U.S. citizens almost certainly violates the law as it currently stands. *See* Elizabeth B. Bazan & Jennifer K. Elsea, Congressional Research Serv., Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information (2006), *available at* http://www.fas.org/sgp/crs/intel/m010506.pdf (providing a detailed analysis of President Bush's executive order allowing domestic wiretapping

The current situation is returning FISA to the spotlight, and many of the Act's more controversial provisions are being reexamined.[6] FISA was passed in order to provide the executive branch with a quick and secure means of satisfying the Fourth Amendment's warrant requirement for domestic investigations related to foreign intelligence and counterterrorism.[7] The Act primarily controls the government's surveillance of domestic communications involving U.S.

---

without a court order and concluding that courts likely will find the program to be inconsistent with federal law); Letter from Curtis A. Bradley, Richard & Marcy Horvitz Professor of Law, Duke Univ., et al., to the Honorable Bill Frist, Majority Leader, U.S. Senate, et al. (Jan. 9, 2006), *available at* http://www.cdt.org/security/20060109legalexpertsanalysis.pdf (concluding that President Bush's executive order is unlawful); *see also* FISA, 50 U.S.C. § 1809(a) (2000) ("A person is guilty of an offense if he intentionally engages in electronic surveillance under color of law except as authorized by statute . . . ."); Authorization for Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001) (codified at 50 U.S.C. § 1541 note (2000 & Supp. III 2003)) ("[T]he President is authorized to use all *necessary and appropriate* force against those nations, organizations, or persons *he determines planned, authorized, committed, or aided* the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations, or persons.") (emphasis added); *Keith*, 407 U.S. at 321 (reasoning that the CIA may not conduct domestic surveillance for national security purposes without a warrant); Katz v. United States, 389 U.S. 347, 357 (1967) ("'Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,' and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment . . . .") (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951) (citation omitted)); Youngstown Sheet & Tube Co. v. Sawyer (*Steel Seizure*), 343 U.S. 579, 637 (1952) (Jackson, J., concurring) (reasoning that the President's authority to protect national security is at its lowest ebb whenever the President seeks to act in violation of an act of Congress); Tom Daschle, Editorial, *Power We Didn't Grant*, WASH. POST, Dec. 23, 2005, at A21 (stating that not only did Congress not intend the Authorization for Use of Military Force (the "AUMF") to allow warrantless surveillance within the United States, but also that such broad domestic authority was specifically requested prior to the AUMF's passage and that request was denied).

[6] *See* Mark Moller, *Untwist the Chain of Command*, LEGAL TIMES, Feb. 28, 2006, *available at* http://www.law.com/jsp/dc/PubArticleDC.jsp?id=1141047297225 (detailing various perspectives on the procedural framework established under FISA); *see also* Jerry Crimmins, *NSA Wiretaps Debated at U of Chicago*, CHI. DAILY L. BULL., Feb. 1, 2006, at 1 (detailing a discussion held at the University of Chicago Law School between University of Chicago Law Professor Geoffrey R. Stone and Seventh Circuit Judge Richard A. Posner regarding warrantless NSA surveillance and the efficacy of FISA's provisions); Patricia Manson, *Bar Group to Debate Curbs on Federal Surveillance Activities*, CHI. DAILY L. BULL., Feb. 10, 2006, at 1 (stating that U.S. Representative Heather Wilson, R-N.M., had called for a full review of the NSA warrantless domestic surveillance program and mentioning the possibility of new legislation that would amend FISA's provisions).

[7] S. REP. NO. 95-604, at 15 (1977); *see also* Susan Goering, *An Unnecessary Breach of Law*, BALT. SUN, Dec. 21, 2005, at 19A (discussing the compliant nature of the Foreign Intelligence Surveillance Court, and stating that out of the 18,747 warrant petitions received by the court from 1979 to 2005, only four were rejected).

citizens or permanent residents;[8] it does not limit electronic surveillance of any communications between aliens outside the United States.[9] The NSA may freely surveil such conversations with virtually no limitations under U.S. law.[10]

FISA maintains a strict distinction between purely domestic calls between U.S. persons, and purely foreign communications between non-U.S. persons outside the United States.[11] Surveillance of the former always requires approval from the Foreign Intelligence Surveillance Court, whereas surveillance of the latter never requires such approval.[12] A substantial gray area exists when calls are placed from within the United States to non-U.S. persons abroad. Non-U.S. persons outside the United States may be freely surveilled by the NSA without even a FISA warrant; therefore, when an unidentified U.S. person places a call to an alien outside the United States who is being surveilled by the NSA lawfully without a warrant, the NSA then automatically and inadvertently surveils that U.S. person. In such a situation, serious questions arise as to the extent to which information

---

[8] FISA's provisions require the government to obtain a FISA warrant when seeking to surveil a "United States person." A U.S. person is defined as a U.S. citizen, a permanent resident, a corporation incorporated in the United States, or an unincorporated association consisting of mostly U.S. citizens or permanent residents. FISA, 50 U.S.C. § 1801(i) (2000).

[9] FISA does not apply to surveillance activities conducted outside the United States. Title I of FISA contains all of the Act's substantive provisions and is titled, "Electronic Surveillance *Within the United States* for Foreign Intelligence Purposes." FISA, Pub. L. No. 95-511, §§ 101–111, 92 Stat. 1783, 1783–96 (codified at 50 U.S.C. §§ 1801–1811 (2000 & Supp. III 2003)) (emphasis added). In addition, the term "electronic surveillance" is defined under the Act so as to exclude surveillance activities that take place outside the United States. FISA § 101, 50 U.S.C. § 1801(f) (2000 & Supp. III 2003).

[10] The Fourth Amendment does not place any restraints on the power of the government to surveil non-U.S. persons outside the United States. United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990) (holding that aliens outside U.S. territory are not entitled to any protection under the Fourth Amendment).

[11] *See* FISA, 50 U.S.C. § 1801(i) (defining "United States person" as "a citizen of the United States, an alien lawfully admitted for permanent residence, . . . an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power").

[12] FISA allows non-U.S. persons to be surveilled in the United States without a FISA warrant based solely upon certification by the Attorney General. *See* FISA, 50 U.S.C.A. § 1802(a) (West 2001 & Supp. 2005). If, however, there is a substantial likelihood that a U.S. person's communication will be surveilled in the course of these efforts, the government must seek approval from the Foreign Intelligence Surveillance Court. *See* FISA, 50 U.S.C. § 1802(b); *see also* FISA, 50 U.S.C.A. § 1804 (detailing the requirements for FISA warrant applications).

gained from such efforts may be used subsequently against that U.S. person.

The NSA's attempt to answer these questions can be found in the agency's minimization procedures, which are detailed in United States Signals Intelligence Directive 18 ("USSID 18").[13] Under most circumstances, the directive requires the NSA to destroy information gained inadvertently from unsuspecting U.S. persons without a warrant;[14] however, section 7.2(c)(4) allows the agency to disseminate such "inadvertently acquired" information to U.S. law enforcement if it appears to implicate the U.S. person in criminal conduct.[15]

This Article discusses this loophole in light of recent advancements in encrypted Voice over Internet Protocol ("VoIP") technology. It concludes that the minimization procedures set forth in USSID 18 are constitutionally deficient because they fail to take into account the growing expectation of privacy that has resulted from advancements in encryption technology. The directive should be redrafted to mandate greater consideration of an individual's reasonable expectation of privacy when determining how information collected without a warrant may be disseminated and used by the agency.

This Article is comprised of four parts. Part I provides an explanation of the NSA and its signals intelligence activities.[16] Part II discusses the legal framework for the electronic surveillance operations of the NSA and explains the loophole that allows the agency to seize and analyze international communications made by U.S. citizens without a warrant.[17] Part III examines encrypted Internet telephony, cryptanalysis, and the territorial limits of constitutional rights.[18] Part IV discusses the constitutionality of section 7.2(c)(4) of USSID 18 as applied to encrypted Internet telephony.[19] The Article then concludes by proposing that communication via encrypted Internet telephony offers the user such a reasonable expectation of privacy that the Fourth Amendment should extend to prevent dissemination of information pertaining to U.S. persons gained from the warrantless

---

[13] Nat'l Sec. Agency/Cent. Sec. Serv., United States Signals Intelligence Directive 18, (July 27, 1993) [hereinafter USSID 18], *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-02.htm (declassified version with some language redacted by the NSA).

[14] *Id.* § 3.1.

[15] *Id.* § 7.2(c)(4).

[16] *See infra* notes 21–50 and accompanying text.

[17] *See infra* notes 51–144 and accompanying text.

[18] *See infra* notes 145–191 and accompanying text.

[19] *See infra* notes 192–232 and accompanying text.

capture of such communications—except in very limited situations where truly exigent circumstances exist.[20]

I. Background: Signals Intelligence and the NSA

Signals intelligence, or SIGINT, refers to intelligence acquired through the capture of electronic signals.[21] The term encompasses three categories of intelligence information: communications intelligence ("COMINT"); electronics intelligence ("ELINT"); and foreign instrumentation signals intelligence ("FISINT").[22] The NSA is the agency responsible for the signals intelligence operations of the United States.[23] In addition to the initial gathering of signals, SIGINT operations often involve subsequent cryptanalysis[24] which is performed by the Central Security Service (the "CSS"),[25] a component sub-agency of the NSA that brings together the cryptographic and cryptanalytic capabilities of the Army, Navy, Marines, and Air Force.[26]

Although the scope of the NSA's SIGINT operations has always been the subject of wild speculation, the true number of communications intercepted by the agency has remained a closely guarded secret. Speculation about the number of communications intercepted by the NSA began to grow when rumors of a global signals intelligence network involving multilateral cooperation between several nations be-

---

[20] *See infra* notes 225–238 and accompanying text.

[21] The term "signals intelligence" or "SIGINT" describes the broad practice of intelligence gathering through various electronic means. *See* U.S. Dep't of Defense, Directive No. 5100.20, ¶ 3.1 (Dec. 23, 1971) (as amended through June 24, 1991), *available at* http://www.dtic.mil/whs/directives/corres/pdf2/d510020p.pdf.

[22] *See id.* "Communications intelligence" or "COMINT" is a subset of the broader discipline of signals intelligence that deals specifically with the capture of encrypted communications for intelligence purposes. Although "communications intelligence" is probably a more apt description of the specific type of operations at issue in this Article, the term is often used interchangeably with "signals intelligence" in common parlance, so I have chosen to use the latter throughout this Article to be certain to cover all relevant NSA operations.

[23] Exec. Order No. 12,333, § 1.12(b)(1), 3 C.F.R. 200, 208 (1982) ("No other department or agency may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense . . . ."), *reprinted in* 50 U.S.C. § 401 note (2000).

[24] Cryptanalysis is defined as "[t]he conversion of encrypted messages into plain text without having the initial knowledge of the key used in encryption." Nat'l Sec. Agency/Cent. Sec. Serv., Frequently Asked Questions About NSA, http://www.nsa.gov/about/about00018.cfm#18 (last visited Mar. 23, 2006).

[25] Although the combined National Security Agency and Central Security Service are often referred to as the NSA/CSS, the two entities will be discussed collectively as the "NSA" throughout most of this Article for the purpose of simplicity.

[26] Nat'l Sec. Agency/Cent. Sec. Serv., *supra* note 24.

gan to surface in 1988. In that year, Margaret Newsham, a former contract employee working at the NSA field station in Menwith Hill, Yorkshire, England,[27] complained to the U.S. House Permanent Select Committee on Intelligence about alleged corruption and impropriety surrounding the use of the NSA's signals intelligence resources.[28] She claimed to have witnessed employees of the agency intercepting a telephone call placed by then-U.S. Senator Strom Thurmond.[29] Her allegations also included details of a global surveillance system known as ECHELON.[30] This fueled public interest and a large number of newspaper articles, but the agency remained silent about the system, and media coverage fizzled shortly thereafter.[31]

In recent years, several high-profile investigative reports have rekindled public interest in the ECHELON network. For example, in 2000, the CBS program *60 Minutes* aired a feature on the ECHELON system.[32] The program included an interview with Mike Frost, a former twenty-year employee of Canada's principal signals intelligence agency, the Communications Security Establishment (the "CSE").[33] During the interview, Frost made revelations about the specific capabilities of the ECHELON system, stating at one point that the system captures "everything . . . from data transfers to cell phones to portable phones to baby monitors to ATMs."[34] Frost had been one of the first insiders to divulge specifics about the breadth of ECHELON's surveillance capabilities, and his account helped to spark renewed public interest in the system.[35]

---

[27] The NSA's Menwith Hill Station in Yorkshire, England, is rumored to be the largest signals intelligence facility in the world. *60 Minutes: ECHELON; Worldwide Conversations Being Received by the ECHELON System May Fall into the Wrong Hands and Innocent People May Be Tagged as Spies* (CBS television broadcast Feb. 27, 2000) [hereinafter *60 Minutes*].

[28] Duncan Campbell, Making History: The Original Source for the 1988 First ECHELON Report Steps Forward, Feb. 25, 2000, http://cryptome.org/echelon-mndc.htm.

[29] *Id.*

[30] *See id.*

[31] *See generally* Mike Frost, Spyworld: Inside the Canadian & American Intelligence Establishments (1994) (giving Frost's first account of some of the operations of Canada's Communications Security Establishment (the "CSE") and the NSA).

[32] *60 Minutes*, *supra* note 27.

[33] *Id.*

[34] *Id.*

[35] *See generally* Frost, *supra* note 31 (offering an account of the operations between the CSE and the NSA). Although much of the controversy surrounding ECHELON is relatively recent, multilateral SIGINT collaboration between these nations is nothing new. Their cooperation began with the BRUSA COMINT Alliance between the United States and the British Commonwealth, which was created at the end of World War II. *See* Lawrence D. Sloan, Note, *ECHELON and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 Duke L.J.

News reports concerning the ECHELON system raised concerns in Europe, and on July 5, 2000, the European Parliament established a temporary committee to investigate.[36] Approximately one year later, this committee issued its "Report on the Existence of a Global System for the Interception of Private and Commercial Communications."[37] The report detailed the existence of ECHELON, its legality under European and international law, and its implications for the privacy rights of European citizens.[38] Subsequently, the European Union began seeking ways to counter the effects of ECHELON through enhanced encryption protocols.[39] In 2004, the European Union created the SECOQC project.[40] Under the project, the European Union will spend €11 million on research and development for a new quantum encryption system that could be used to thwart the signals intelligence capabilities of ECHELON.[41]

The ECHELON system is rumored to capture as many as three billion communications each day.[42] The system's reach spans the globe due to the strategic locations of its five member nations, which

---

1467, 1471 (2001) (discussing the origins of UKUSA SIGINT cooperation); *see also* Simon Chesterman, Shared Secrets: Intelligence and Collective Security 22 (Lowy Inst. Paper No. 10, 2006), *available at* http://www.lowyinstitute.org/Publication.asp?pid=360 (providing a detailed history of UKUSA signals intelligence cooperation); Stephen Fidler & Mark Huband, *A Special Relationship? The US and UK Spying Alliance Is Put Under the Spotlight*, Fin. Times, July 6, 2004, at 17 (providing additional details about the nature of cooperation between the NSA and the United Kingdom's Government Communications Headquarters (the "GCHQ")).

[36] Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System), Eur. Parl. Doc. A5-0264/2001 final (2001) [hereinafter E.U. Report], *available at* http://www.fas.org/irp/program/process/rapport_echelon_en.pdf.

[37] *Id.*

[38] *Id.*

[39] *See* Philip Willan, E.U. Seeks Quantum Cryptography Response to Echelon, May 17, 2004. http://security.itworld.com/4361/040517euechelon/page_1.html.

[40] SECOQC Stands for Secure Communication Based on Quantum Cryptography. SECOQC Home Page, http://www.secoqc.net (last visited Mar. 23, 2006).

[41] *See* Chesterman, *supra* note 35, at 21 (discussing the European Union's efforts to secure communications through quantum cryptography); *see also* Willan, *supra* note 39, (discussing the European Union's plans to develop a secure communication system that would be immune from the interception capabilities of ECHELON). This move by the European Union seems to be fueling competition between technology firms to develop new and better forms of data encryption. *See* R. Colin Johnson, *Quantum Encryption Enters Product Phase*, Electronic Engineering Times, May 2, 2005, at 44 (discussing the Infosecurity Europe 2005 trade show in London, where a new turnkey quantum encryption system and other encryption innovations were unveiled).

[42] Vernon Loeb, *Critics Questioning NSA Reading Habits; Politicians Ask if Agency Sweeps in Private Data*, Wash. Post, Nov. 13, 1999, at A3.

include the United States, the United Kingdom, Canada, Australia, and New Zealand.[43] Together, these nations comprise the UKUSA community, which has its roots in the BRUSA COMINT alliance established between the United States and the British Commonwealth during World War II.[44] Through satellite and other means, ECHELON is believed to be capable of capturing most electronic signals broadcast anywhere in the world.[45]

The NSA has refused to comment on ECHELON, even invoking attorney-client privilege to avoid compliance with document requests made by the U.S. House Permanent Select Committee on Intelligence.[46] Such actions have fueled speculation by conspiracy theorists, as well as concern on the part of civil libertarians.[47] Although most estimates about the exact capabilities of ECHELON are likely exaggerated by these groups, the amount of data collected by the joint efforts of the UKUSA community is probably much more substantial than imagined before the existence of ECHELON came to light.[48] Consequently, due to the large volume of international communications potentially being captured by ECHELON, there is a substantial likelihood

---

[43] There are five agencies that participate in collective signals operations through the ECHELON network. They are the United States' NSA, the United Kingdom's GCHQ, Canada's CSE, Australia's Defence Signals Directorate ("DSD"), and New Zealand's Government Communications Security Bureau ("GCSB"). *See* CHESTERMAN, *supra* note 35, at 22; *see also* Sloan, *supra* note 35, at 1471 (discussing the global reach of ECHELON that results from multinational, cooperative intelligence gathering).

[44] E.U. Report, *supra* note 36, at 60–61; *see also* CHESTERMAN, *supra* note 35, at 22 (providing a detailed history of UKUSA signals intelligence cooperation).

[45] *See* E.U. Report, *supra* note 36, at 34.

[46] On August 31, 1999, U.S. Representative Bob Barr (R-Ga.) was interviewed by Fox News host Bill O'Reilly and was asked about the House Intelligence Committee's attempts to discover more information about the ECHELON network. He stated that "when the House Intelligence Committee did ask the NSA for the justification and an explanation of this program, not only did they refuse to give it to them, but—get this—their rationale was 'We can't give it to you because that's attorney-client privilege.'" *The O'Reilly Factor: Unresolved Problem: Project ECHELON* (Fox News Channel television broadcast Aug. 31, 1999); *see also* John C. K. Daly, *ECHELON—The Ultimate Spy Network?*, UNITED PRESS INT'L, Mar. 1, 2004 (describing the U.S. government's "terse 'no comment' attitude to all inquiries regarding Echelon").

[47] Many civil liberties groups have expressed concern over the NSA's reluctance to reveal details about the operation of the ECHELON system. After the NSA's refusal to disclose documents, the American Civil Liberties Union, the Electronic Privacy Information Center, and the Omega Foundation created EchelonWatch.org, a website dedicated to tracking the system. *See* Robert MacMillan, *ACLU Plans to Observe Echelon Global Spy Net Online*, NEWSBYTES, Nov. 16, 1999.

[48] *See* E.U. Report, *supra* note 36, at 34 ("If UKUSA States operate listening stations in the relevant regions of the earth, in principle they can intercept all telephone, fax, and data traffic transmitted via such satellites.").

that a significant number of international phone calls made to and from American citizens were being collected by the NSA even before President Bush issued his secret executive order.[49] The next Part details the legal structure that regulates the NSA's signals intelligence efforts and describes the situations where U.S. citizens might have their conversations monitored by the agency without a warrant.[50]

II. The Legal Framework Governing NSA SIGINT Operations

The NSA's electronic surveillance activities are governed primarily by four authorities: the U.S. Constitution,[51] FISA,[52] Executive Order No. 12,333,[53] and USSID 18.[54] The Fourth Amendment and FISA provide a high degree of protection for U.S. persons inside the United States and a slightly lower degree of protection for U.S. persons located outside U.S. borders.[55] With the exception of some rules related to diplomatic personnel, non-U.S. persons located outside the United States are offered practically no protection from electronic

---

[49] Even prior to the controversial order, it was possible for the NSA to keep and disseminate information collected about U.S. citizens although no warrant authorized the initial surveillance. *See* USSID 18, *supra* note 13, § 3.1.

[50] *See infra* notes 51–144 and accompanying text.

[51] *See* U.S. Const. amend. IV.

[52] *See* FISA, 18 U.S.C.A. §§ 2511, 2518, 2519, 50 U.S.C.A. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871 (West 2001 & Supp. 2005).

[53] *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 note (2000).

[54] *See* USSID 18, *supra* note 13.

[55] Courts have held that the government may use evidence collected by foreign governments against U.S. persons at trial in the United States even though such evidence was collected in a manner that would have violated their constitutional rights if conducted by U.S. agents. *See* Stefan Epstein, Annotation, *Application of Fourth Amendment Exclusionary Rule to Evidence Obtained Through Search Conducted by Official of Foreign Government*, 33 A.L.R. Fed. 342, § 3(a) (1977) (explaining the general rule that the exclusionary rule does not apply to searches conducted by foreign governments). This is true even if U.S. agents are involved with the foreign government's efforts, provided that their participation is not substantial. *See id.*; *see also* Gov't of Canal Zone v. Sierra, 594 F.2d 60, 72 (1979) ("Fourth Amendment rights are generally inapplicable to an action by a foreign sovereign in its own territory in enforcing its own laws, even though American officials are present and cooperate in some degree."). Also, traffic stops and questioning conducted by U.S. border officials on U.S. citizens entering and leaving the country have been upheld as constitutional despite the absence of probable cause or reasonable suspicion. United States v. Martinez-Fuerte, 428 U.S. 543, 566 (1976) (holding that the use of fixed border checkpoints and the questioning of travelers at U.S. borders do not require warrants or probable cause). The Supreme Court has also held that the government may hand over an American soldier for trial by a foreign government although U.S. constitutional guarantees will not be provided. Wilson v. Girard, 354 U.S. 524, 530 (1957).

surveillance by U.S. intelligence agencies.[56] Therefore, international telephone calls from U.S. citizens inside the United States to foreign acquaintances abroad could be captured by the NSA without a warrant if those foreign acquaintances are under NSA surveillance. In such a situation, the only protections currently afforded to U.S. citizens are found in the minimization procedures mandated by FISA[57] and Executive Order No. 12,333.[58] The specific minimization procedures applicable to NSA operations are detailed in USSID 18.[59] Each of the four legal authorities—and the protections they provide—are discussed individually below.

A. *The Fourth Amendment*

The Fourth Amendment to the U.S. Constitution lays the foundation for all legal restrictions on the NSA's electronic surveillance and signals intelligence operations.[60] It ensures the right of U.S. persons to be free from unreasonable searches and seizures, and mandates that no warrants be issued absent a showing of probable cause.[61] Prior to 1967, electronic surveillance was not considered to be a "search" for purposes of the Fourth Amendment.[62] However, in 1967, the Supreme Court extended the definition to include electronic surveillance, thereby requiring all government agencies to obtain a warrant prior to conducting such surveillance on U.S. persons.[63]

---

[56] International law places restrictions on the ability of governments to surveil diplomatic missions within their territory. Vienna Convention on Diplomatic Relations and Optional Protocol on Disputes art. 22, Apr. 18, 1961, 23 U.S.T. 3227, 500 U.N.T.S. 95 (stating that the premises of diplomatic missions are inviolable and immune from search). A host nation may not interfere with the official correspondence of a diplomatic mission. *Id.* art. 27. United Nations diplomats and officials are also afforded protection from surveillance under international law. *See* Convention on the Privileges and Immunities of the United Nations art. 2, § 3, Apr. 29, 1970, 21 U.S.T. 1418, 1 U.N.T.S. 16 (providing that the premises of the United Nations are inviolable and are immune from search); *see also* Agreement Between the United Nations and the United States of America Regarding the Headquarters of the United Nations, June 26, 1947, 61 Stat. 3416, 11 U.N.T.S. 11 (same).

[57] FISA, 18 U.S.C.A. §§ 2511, 2518, 2519, 50 U.S.C.A. §§ 1801–1811, 1821–1829, 1841–1846. 1861–1862, 1871 (West 2001 & Supp. 2005).

[58] Exec. Order No. 12,333, §§ 2.3–2.4, 3 C.F.R. 200, 211–12 (1982), *reprinted in* 50 U.S.C. § 401 note (2000).

[59] USSID 18, *supra* note 13.

[60] *See* U.S. CONST. amend. IV.

[61] *Id.* ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation . . . .").

[62] *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

[63] Katz v. United States, 389 U.S. 347, 359 (1967).

The rights protected by the Fourth Amendment are subject to some important limitations. For example, since World War II, U.S. presidents have asserted that the executive branch has the power to order warrantless electronic surveillance when national security is at stake.[64] This exception has become known as the national security exception to the Fourth Amendment.[65] Although the exception is not specifically enumerated in the Constitution, caselaw has recognized a limited set of circumstances under which the President's power to control foreign affairs mav allow warrantless searches to be ordered to effectuate that purpose.[66] Courts have, however, allowed the exception to be invoked only in a limited set of situations, all of which have involved some form of foreign security effort.[67] Moreover, the Supreme Court has specifically refused to recognize the national security exception in cases involving domestic surveillance operations targeting American citizens within U.S. borders.[68] For instance, in 1972, in *United States v. U.S. District Court (Keith)*, the Supreme Court held that the President's power to protect national security did not eliminate the need for the Central Intelligence Agency to obtain a warrant before conducting electronic surveillance of suspected terrorists within the territorial boundaries of the United States.[69] This holding proved

---

[64] *See* Michael A. DiSabatino, Annotation, *Construction and Application of "National Security" Exception to Fourth Amendment Search Warrant Requirement*, 39 A.L.R. Fed. 646, § 2a (1978).

[65] *See id.*

[66] *See* 68 Am. Jur. 2d *Searches and Seizures* § 161 (2005); *see also* United States v. Totten, 92 U.S. 105, 106 (1875) (recognizing the President's power to conduct foreign affairs includes the power to authorize foreign intelligence operations and the use of clandestine agents); United States v. Sinclair, 321 F. Supp. 1074, 1079 (E.D. Mich. 1971) ("Presidential power of surveillance is specifically limited to 'exceptional cases'—cases of a non-criminal nature or which concern the country's national security.").

[67] *See* 68 Am. Jur. 2d *Searches and Seizures* § 161 (2005) ("Generally, there is no clearly announced 'national security' exception to the requirement of a search warrant. To the extent there is such an exception, it may only be invoked by the special authorization of the President or the Attorney General of the United States. The distinguishing element between domestic security cases, in which no exception to the warrant requirement exists, and cases involving foreign security, in which an exception may exist, is whether the activities of the subject at which the search is directed affect the foreign relations of the United States.") (footnotes omitted). *Compare* United States v. Ehrlichman, 376 F. Supp. 29, 35 (D.D.C. 1974) (refusing to recognize a broad interpretation of the national security exception), *with* United States v. Butenko, 494 F.2d 593, 605–06 (3d Cir. 1974) (holding that a warrant was not required in a case involving surveillance conducted for foreign intelligence purposes, but reasoning that if members of a domestic political organization were the subject of such surveillance unrelated to foreign affairs, such surveillance would "undoubtedly" be illegal).

[68] *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 315–16 (1972).

[69] *Id.*

problematic for U.S. intelligence agencies, which feared that seeking a warrant through traditional avenues would require divulging secret information about agency methods and ongoing operations.[70] The *Keith* Court had, however, specifically refused to address the issue of whether the agency was required to obtain a traditional warrant in matters involving foreign powers or agents,[71] which left room for Congress to step in and create an alternative means of satisfying the warrant requirement while also protecting classified information.[72]

Accordingly, with FISA's passage in 1978, Congress provided U.S. agencies with an alternative means of obtaining warrants for foreign intelligence surveillance operations targeting U.S. persons.[73] Another purpose of the Act was to prevent abuses by the executive branch, which had engaged in domestic surveillance of civil rights and antiwar activists during the Vietnam era.[74] FISA established strict procedural rules for conducting electronic surveillance for foreign intelligence and counterintelligence purposes within the United States.[75]

It is important to note that FISA does not apply to foreign surveillance operations that target non-U.S. persons located abroad.[76] FISA merely provides a procedural framework for satisfying the requirements of the Fourth Amendment, and the Fourth Amendment does not extend protection to non-U.S. persons outside the territorial limits of the United States.[77] The Supreme Court reiterated and strengthened this stance in 1990, when it held that the Fourth Amendment does not even protect against warrantless property seizures by U.S. agents against for-

---

[70] *See id.* at 319 (quoting a brief for the United States as stating that being required to obtain search warrants in these cases would require disclosures to magistrates that "would create serious potential dangers to the national security and to the lives of informants and agents").

[71] In *Keith*, the Supreme Court held that the government was required to obtain a warrant to conduct domestic surveillance related to national security, but it refused to address the issue of a warrant requirement for foreign cases. Specifically, the Court stated, "this case involves only the domestic aspects of national security. We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents." *Id.* at 321–22.

[72] *See id.*; *cf.* Zweibon v. Mitchell, 516 F.2d 594, 654–55 (D.C. Cir. 1975) (refusing to extend the national security exception to allow a warrantless search of people who were not agents of a foreign power).

[73] *See* S. REP. NO. 95-604, at 15 (1977).

[74] *See id.*; Risen & Lichtblau, *supra* note 2, at A1.

[75] *See* FISA, 18 U.S.C.A. §§ 2511, 2518, 2519, 50 U.S.C.A. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871 (West 2001 & Supp. 2005).

[76] *See* 50 U.S.C. § 1801(f) (2000 & Supp. III 2003).

[77] United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990).

eign nationals abroad.[78] Therefore, there are virtually no constitutional limits on the ability of the NSA—or any other U.S. agency—to conduct electronic surveillance or even property seizures on non-U.S. persons abroad.[79] Consequently, FISA's warrant requirement does not apply to situations where a non-U.S. person is the target of NSA surveillance outside the United States, even if U.S. persons may be inadvertently surveilled as a result.[80]

B. *The Foreign Intelligence Surveillance Act of 1978*

FISA applies to all instances of electronic surveillance performed by government agents within the United States for foreign intelligence purposes.[81] Its procedural framework is distinct from that governing the conduct of electronic surveillance for general law enforcement purposes,[82] which is instead governed primarily by two other congressional acts: Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III")[83] and the Electronic Communications Privacy Act of 1986 (the "ECPA").[84] Title III was passed in 1968 in order to regulate surveillance of oral communications. Additionally, in 1986, Congress passed the ECPA, which amended Title III and extended its scope to cover the new forms of electronic communication presented by increased computer usage.[85] These two statutes provide guidance to U.S. law enforcement and intelligence agencies seeking to conduct domestic surveillance for law enforcement purposes. Although some assistance is allowed, the NSA is generally not permit-

---

[78] *See id.*

[79] *See id.* (holding that the Fourth Amendment does not apply to physical searches or seizures against non-U.S. persons located outside the United States); *see also* United States v. Truong Dinh Hung, 629 F.2d 908, 915–16 (4th Cir. 1980) (upholding the warrantless surveillance of a non-U.S. citizen who was an agent of the Vietnamese government).

[80] *See Verdugo-Urquidez*, 494 U.S. at 274–75; *Truong Dinh Hung*, 629 F.2d at 915–16.

[81] *See* FISA, 50 U.S.C.A. §§ 1801(f), 1804(a)(7)(B) (West 2001 & Supp. 2005).

[82] *See* S. Rep. No. 95-604, at 15 (1977).

[83] Pub. L. No. 90-351, § 802, 82 Stat. 197, 212–23 (codified as amended at 18 U.S.C. §§ 2510–2520 (2000 & Supp. III 2003)).

[84] Pub. L. No. 99-508, § 201(a), 100 Stat. 1848, 1861–63 (codified as amended at 18 U.S.C. § 2703 (2000 & Supp. III 2003)). Congress passed the ECPA in 1986 in order to respond to the increasing use of computers to transmit private data and communications. The advent of the Internet made it necessary to update the previous classifications under the Omnibus Crime Control and Safe Streets Act of 1968, which had limited the definition of wire tapping to traditional phone calls. The ECPA extended protection to these electronic communications. *See* 132 Cong. Rec. H8977 (daily ed. Oct. 2, 1986) (statement of Rep. Kastenmeier).

[85] *See* 132 Cong. Rec. H8977 (daily ed. Oct. 2, 1986) (statement of Rep. Kastenmeier) (explaining the purpose of the ECPA).

ted to conduct signals intelligence operations within the United States for the purpose of general domestic law enforcement.[86] NSA operations are typically confined to foreign intelligence, counterintelligence, or counterterrorism purposes.[87] As a result, the NSA's domestic ECHELON operations are primarily governed by FISA.

Although the NSA is not generally permitted to conduct domestic surveillance for law enforcement purposes, information about U.S. citizens obtained under a FISA warrant may be used in criminal proceedings against them.[88] The information sought to be used need not be evidence of a crime related to espionage. The only limitation is that the collection of foreign intelligence information must have been a "significant" purpose of the FISA surveillance.[89] Prior to the passage of the USA PATRIOT Act in 2001,[90] the collection of foreign intelligence in-

---

[86] USSID 18, *supra* note 13, § 1.4 ("[T]he focus of all foreign intelligence operations is on foreign entities and persons."). However, NSA assistance to law enforcement is permitted in a limited number of circumstances. *See* 10 U.S.C. § 371 (2000) (permitting the Secretary of Defense to provide law enforcement agencies with information collected by Department of Defense components if that information is relevant to narcotics trafficking).

[87] USSID 18, *supra* note 13, § 3.1 ("The policy of the [U.S. SIGINT System] is to target or collect only foreign communications. The USSS will not intentionally collect communications to, from or about U.S. persons or persons or entities in the U.S. except as set forth in this [U.S. Signals Intelligence Directive].").

[88] *See* 50 U.S.C.A. § 1804(a)(7)(B) (West 2001 & Supp. 2005).

[89] Originally, FISA required the collection of foreign intelligence information to be the primary purpose of FISA-related surveillance. FISA, Pub. L. No. 95-511, § 104(a)(7)(B), 92 Stat. 1783, 1789 (1978) (codified at 50 U.S.C. § 1804(a)(7)(B) (1982)). However, the USA PATRIOT Act amended this requirement. Under the new language, the collection of foreign intelligence information need only be a "significant purpose" of the proposed surveillance for a FISA warrant to be issued. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (2001) (codified at 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B) (2000 & Supp. III 2003)). Originally, this new definition was set to expire on December 31, 2005. *Id.* § 224, 115 Stat. at 295 (codified at 18 U.S.C. § 2510 note (2000 & Supp. III 2003)), *repealed by* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 102, 120 Stat. 192 (2006). Congress extended this date to March 10, 2006 in order to allow more time to debate. *See* Sheryl Gay Stolberg, *Key Senators Reach Accord on Extending the Patriot Act*, N.Y. TIMES, Feb. 10, 2006, at A14. On March 2, 2006, the Senate voted for a permanent extension to this provision, making the new language permanent. *See* Sheryl Gay Stolberg, *Senate Passes Legislation to Renew Patriot Act*, N.Y. TIMES, Mar. 3, 2006, at A14. The House of Representatives voted in favor of the bill on March 7, 2006. *See* Sheryl Gay Stolberg, *Patriot Act Revisions Pass House, Sending Measure to President*, N.Y. TIMES, Mar. 8, 2006, at A20. President George W. Bush signed the permanent extension into law on March 9, 2006—just one day before the provision would have expired. *See* John Diamond, *Bush Makes Patriot Provisions Permanent*, USA TODAY, Mar. 10, 2006, at 6A; *see also* USA PATRIOT Improvement and Reauthorization Act of 2005 § 102.

[90] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 106-56, 115 Stat. 272 (codified as

formation needed to be the "primary purpose" of FISA surveillance. Now, it need only be a "significant purpose" of the surveillance in order for a FISA warrant to be issued.[91] This change drastically increased the ease with which government agents can obtain domestic surveillance warrants under FISA.

FISA was intended to govern every instance of electronic surveillance conducted by U.S. agents within the territorial boundaries of the United States for foreign intelligence or counterintelligence purposes.[92] Section 201(b) of the Act states that FISA "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire and oral communications may be conducted."[93] The Act set forth procedures through which the government may seek authorization for such surveillance without being required to follow the traditional warrant procedures mandated by the Fourth Amendment.[94] Congress believed this step was necessary to protect sensitive national security information that might otherwise be revealed under the traditional warrant issuance framework.[95]

---

amended in scattered sections of 8 U.S.C., 12 U.S.C., 15 U.S.C., 18 U.S.C., 20 U.S.C., 21 U.S.C., 22 U.S.C., 28 U.S.C., 31 U.S.C., 42 U.S.C., 47 U.S.C., 49 U.S.C., 50 U.S.C.).

[91] FISA, 50 U.S.C. § 1804(a)(7) (2000 & Supp. III 2003) (stating that applications for FISA warrants must include a certification by an executive branch official verifying that "the certifying official deems the information sought to be foreign intelligence information" and that "a significant purpose of the surveillance is to obtain foreign intelligence information").

[92] FISA, 18 U.S.C. § 2511(2)(f) (amending the Omnibus Crime Control and Safe Streets Act of 1968 to provide that FISA "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted"). In 1994, FISA was amended to allow the FISC to issue warrants for physical searches as well as electronic surveillance. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807(a)(3), 108 Stat. 3423, 3443–44 (1994) (codified at 50 U.S.C. § 1822 (2000)) (amending FISA to add a new Title III concerning physical searches, giving the President the power to "authorize physical searches without a court order . . . to acquire foreign intelligence information for periods of up to one year").

[93] FISA, § 201(b), 18 U.S.C. § 2511(2)(f).

[94] FISA, 50 U.S.C.A. § 1802 (West 2001 & Supp. 2005) (providing that "the President, through the Attorney General, may authorize electronic surveillance without a court order . . . to acquire foreign intelligence information for periods of up to one year" if certain conditions are fulfilled and certain procedures are followed).

[95] *See* S. REP. No. 95-604, at 15 (1977). For example, when a U.S. intelligence agency decides to conduct electronic surveillance for foreign intelligence or counterintelligence purposes, that decision is usually based on classified information. The traditional process for obtaining a warrant for such searches would almost invariably involve the disclosure of secret information, which would divulge current intelligence collection efforts and methods. An alternative to the traditional warrant procedures was necessary to preserve national security. FISA provided that alternative.

As part of this procedural framework, FISA established a special court known as the Foreign Intelligence Surveillance Court (the "FISC").[96] This court hears most government requests to conduct "electronic surveillance" within the United States for foreign intelligence purposes.[97] The Act also mandated the adoption of minimization procedures to limit the effects of FISA-authorized surveillance on U.S. persons.[98] FISA does not, however, extend protection to non-U.S. persons outside the United States.[99] Collecting signals information outside U.S. borders is not considered "electronic surveillance" under the Act's definition, even if a U.S. person is specifically targeted.[100]

Although NSA collection efforts under FISA may target only those suspected of being agents of a foreign government or terrorist organization, the Act allows the agency to use unrelated information that is inadvertently acquired about U.S. citizens who are not the proper tar-

---

[96] *See* FISA, 50 U.S.C. § 1803 (2000 & Supp. III 2003), *amended by* Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 1071(e), 118 Stat. 3638, 3691, *and* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106, 120 Stat. 192 (2006); *see also* United States v. Hammoud, 381 F.3d 316, 332 (4th Cir. 2004) (providing an explanation of the purposes behind FISA and its procedural framework). Critics claim that the FISC is merely a rubber stamp for U.S. intelligence and law enforcement agencies, citing the fact that the court denied zero petitions out of the 11,883 petitions it heard during its first twenty-one years of operation. *See* Helene E. Schwartz, *Oversight of Minimization Compliance Under the Foreign Intelligence Surveillance Act: How the Watchdogs Are Doing Their Jobs*, 12 RUTGERS L.J. 405, 445 (1981); Sloan, *supra* note 35, at 1496; *see also* Elec. Privacy Info. Ctr., Foreign Intelligence Surveillance Act Orders 1979–2004, http://www.epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Mar. 24, 2006) (demonstrating that from 1979 to 2004, a total of four petitions for FISA warrants were denied, each in 2003).

[97] *See* FISA, 50 U.S.C. § 1803(a) (2000 & Supp. III 2003).

[98] *See* 50 U.S.C. §§ 1801(h), 1802(a)(1)(C), 1804(a)(5).

[99] *See supra* note 9 and accompanying text; *see also* United States v. Bin Laden, 126 F. Supp. 2d 264, 287 n.26 (S.D.N.Y. 2000) (discussing how searches conducted in Kenya are not governed by FISA).

[100] *See* FISA, 50 U.S.C. § 1801(f). Section 1801(f) of FISA defines four types of conduct that are considered "electronic surveillance" under FISA. Signals collection operations that target U.S. persons outside the United States do not fit within any of these four definitions. The first three definitions require the targeted individual to be located inside of the United States to be considered "electronic surveillance." The fourth definition applies only to the use of surveillance devices within the United States. Therefore, the NSA's signals monitoring stations in the United Kingdom, Canada, Australia, and New Zealand are not regulated by FISA. U.S. personnel located at these foreign stations presumably may monitor U.S. persons who are outside the United States, and that conduct technically would not be considered electronic surveillance under FISA's definitions. This highlights the fact that FISA was meant to govern only domestic surveillance taking place within U.S. borders. Although such efforts would not fall under FISA's definition of "electronic surveillance," USSID 18's minimization procedures still would apply and offer some protection to the rights of U.S. persons abroad. *See generally* USSID 18, *supra* note 13.

gets of the surveillance.[101] If the NSA wishes to use such information obtained during FISA-authorized surveillance, it must comply with its own FISA-related minimization procedures, which are located in Annex A to USSID 18.[102] The procedures in Annex A apply only to information acquired during domestic FISA surveillance conducted pursuant to a FISA warrant.[103]

Non-FISA surveillance against non-U.S. persons abroad may be conducted lawfully without a warrant; however, these operations must still be conducted in a manner that minimizes the impact on the rights of unintentionally monitored U.S. persons.[104] In order to use inadvertently acquired information pertaining to U.S. persons gained through warrantless foreign surveillance, the agency must comply with the minimization procedures mandated by Executive Order No. 12,333 and Department of Defense Directive 5240.1.[105]

---

[101] Although FISA requires the use of minimization procedures to limit the impact of authorized surveillance on U.S. persons who are not named as targets, the Act specifically allows evidence of a crime to be disseminated and used by law enforcement. FISA, 50 U.S.C. § 1801(h)(3). Evidence collected pursuant to a valid FISA warrant may be used in criminal proceedings against persons who were not named in the warrant as targets of the authorized surveillance. *See id.* § 1806(g) (stating that a motion to exclude evidence collected pursuant to a FISA warrant shall be denied if the surveillance was lawfully authorized and conducted); *see also* United States v. Isa, 923 F.2d 1300, 1304 (8th Cir. 1991) ("There is no requirement that the 'crime' be related to foreign intelligence."); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) (holding that evidence collected pursuant to a FISA warrant issued against one individual is admissible as evidence against an acquaintance with whom the individual had spoken during the period of the surveillance).

[102] USSID 18, *supra* note 13, at Annex A, app. 1, § 1 ("These procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is collected in the course of electronic surveillance as ordered by the United States Foreign Intelligence Surveillance Court under Section 102(b) or authorized by Attorney General Certification under Section 102(a) of [FISA].").

[103] *Id.*

[104] *See* FISA, 50 U.S.C. § 1801(h) (2000 & Supp. III 2003).

[105] FISA allows the use of information about any U.S. person that is collected pursuant to a FISA warrant provided that such use is conducted in accordance with applicable minimization procedures. *Id.* § 1806(a). FISA applies only to surveillance conducted inside the United States. Executive Order No. 12,333 mandated that additional minimization procedures be implemented in all U.S. intelligence agencies. Exec. Order No. 12,333, § 2.3, 3 C.F.R. 200, 211 (1982), *reprinted in* 50 U.S.C. § 401 note (2000). These minimization procedures apply to all surveillance regardless of its location. *See id.* Directive No. 5240.1 is the Department of Defense's implementation of the Order's requirements. U.S. Dep't of Defense, Directive No. 5240.1 (Apr. 1988) [hereinafter DoD Directive No. 5240.1], *available at* http://www.dtic.mil/whs/directives/corres/pdf/d52401_042588/d52401p.pdf. Directive 5240.1 applies to all intelligence activities of Department of Defense components, including the NSA. *See id.* Regulation No. 5240.1-R is a detailed regulation that implements Directive No. 5240.1, and this document is tied to a previous version

C. *Executive Order No. 12,333*

The lawfully warrantless foreign surveillance activities of the NSA that are not governed by FISA are governed by Executive Order No. 12,333.[106] President Ronald Reagan issued the order in 1981 in an attempt to provide a clear presidential statement about the duties and responsibilities of the agencies involved in the national intelligence effort and to mandate the adoption of internal administrative minimization procedures applicable to all surveillance efforts conducted by members of the U.S. Intelligence Community.[107] Similar executive orders issued by Presidents Ford and Carter during their administrations preceded Executive Order No. 12,333.[108] Unlike its predecessors, however, Executive Order No. 12,333 has remained in force and virtually unchanged since its issuance in 1981.[109] It has represented the principal executive-branch statement regarding the appropriate scope of U.S. intelligence agency operations for the last twenty-five years.[110]

In addition to containing broad pronouncements about the goals and duties of the different components of the U.S. intelligence apparatus, Executive Order No. 12,333 also places specific limitations on the proper means of conducting intelligence collection. For example, it authorizes the NSA, as a member of the U.S. Intelligence Community, to collect and disseminate information about U.S. citizens for foreign intelligence and counterintelligence purposes, but it limits such collection efforts to those conducted in accordance with the procedures set forth by the Director of the NSA and the Attorney General.[111] Further, it gives the Attorney General the power to approve the use of electronic surveillance upon his or her own determination that there is probable cause to believe that the surveillance is to be used against a foreign

---

of Directive No. 5240.1. *See* DoD Reg. No. 5240.1-R, *supra* note 4. These regulations and directives are revised and reissued periodically using the same numbering. The NSA is required to adhere to both Directive No. 5240.1 and Regulation No. 5240.1-R. The agency issued USSID 18 as an agency-level implementation guideline that lists the minimization procedures mandated by both Directive No. 5240.1 and Executive Order No. 12,333. *See* USSID 18, *supra* note 13.

[106] Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 note (2000).

[107] *Id.*

[108] *See* Exec. Order No. 11,905, 3 C.F.R. 90 (1976) (issued by President Ford); Exec. Order No. 12,036, 3 C.F.R. 112 (1978) (issued by President Carter).

[109] *See* Exec. Order No. 12,333, 3 C.F.R. 200 (1982), *reprinted in* 50 U.S.C. § 401 note (2000).

[110] *See id.*, *reprinted in* 50 U.S.C. § 401 note (2000).

[111] *Id.* § 2.3, 3 C.F.R. at 211, *reprinted in* 50 U.S.C. § 401 note (2000).

power or agent.[112] The order also requires, however, the Attorney General to comply with the minimization requirements imposed by FISA.[113]

With respect to ECHELON, the restrictions imposed by Executive Order No. 12,333 and FISA apply only to situations where the NSA seeks to conduct surveillance within the United States or against U.S. persons abroad.[114] Virtually no restrictions are placed on the ability of the agency to conduct such surveillance on non-U.S. persons located outside the territorial limits of the United States.[115] Because the NSA is allowed to conduct virtually unfettered surveillance of foreign persons outside the United States, American citizens may be inadvertently surveilled by the NSA without a warrant whenever they communicate with foreign persons located in other countries.[116] Even assuming that the NSA does not routinely engage in the interception of domestic U.S. signals, the capture of so many foreign communications still results in the collection, without a warrant, of a significant number of phone calls made to and from U.S. persons each year.[117] Presumably, such situations occurred even prior to President Bush's issuance of the secret executive order allowing warrantless domestic surveillance in apparent violation of FISA.[118]

---

[112] *Id.* § 2.5, 3 C.F.R. at 212, *reprinted in* 50 U.S.C. § 401 note (2000).

[113] *See id.*, *reprinted in* 50 U.S.C. § 401 note (2000).

[114] *See* 50 U.S.C. § 1801(f) (2000 & Supp. III 2003); Exec. Order No. 12,333, § 2.4, 3 C.F.R. at 212 , *reprinted in* 50 U.S.C. § 401 note (2000) ("Agencies within the Intelligence Community shall use the least intrusive collection techniques feasible *within the United States or directed at United States persons abroad.*") (emphasis added). Neither FISA nor Executive Order No. 12,333 place restrictions on the NSA's ability to conduct surveillance targeting non-U.S. persons outside the United States provided the surveillance does not impinge upon the rights of any U.S. person. *See* FISA, 50 U.S.C. § 1801(f); Exec. Order No. 12,333, § 2.4. 3 C.F.R. at 212, *reprinted in* 50 U.S.C. § 401 note (2000).

[115] FISA, 50 U.S.C. § 1801(f); Exec. Order No. 12,333, § 2.4, 3 C.F.R. 200, 212 (1982), *reprinted in* 50 U.S.C. § 401 note (2000); *see also Verdugo-Urquidez*, 494 U.S. at 274–75 (reasoning that the Fourth Amendment did not apply to a Mexican citizen when the place searched was in Mexico).

[116] Justice Brandeis' dissent in *Olmstead v. United States* provides an illustration of this point. *See* 277 U.S. at 471–85 (Brandeis, J., dissenting). He explained that

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him.

Id. at 475–76.

[117] *See* Loeb, *supra* note 42, at A3.

[118] *See id.*

Although the likelihood for the warrantless seizure of international communications involving U.S. citizens seems quite high, the agency has adopted internal safeguards to limit the adverse effects of ECHELON's massive signals intelligence operations with respect to the rights of U.S. citizens. These internal safeguards, mandated by both Executive Order No. 12,333[119] and Department of Defense Directive 5240.1,[120] are embodied in USSID 18.[121]

D. *United States Signals Intelligence Directive 18 (USSID 18)*

USSID 18 sets forth the primary operating guidelines that govern the signals intelligence operations of the NSA.[122] FISA and Executive Order No. 12,333 require these "minimization procedures" in order to reduce the "acquisition and retention, and prohibit the dissemination, of nonpublic information concerning unconsenting United States persons."[123] Accordingly, the NSA's primary objective in detailing these procedures is to minimize the impact on U.S. persons caused by the otherwise legitimate warrantless electronic surveillance routinely conducted by the NSA on non-U.S. persons abroad.[124] Fundamentally, USSID 18 is an attempt to strike a balance between the often competing interests of Fourth Amendment privacy guarantees and U.S. national security.[125]

It is the stated policy of the NSA "to target or collect only foreign communications."[126] USSID 18 makes clear that the NSA "will not intentionally collect communications to, from or about U.S. persons or persons or entities in the United States," except as allowed under its provisions.[127] Although the NSA generally may not intentionally collect the communications of U.S. persons without a FISA warrant, USSID 18 specifically states that the agency may collect such communications unintentionally.[128] More specifically, section 3.1 of USSID 18 states that if the NSA "inadvertently" collects communications made to or from U.S. persons who were not the lawful target of the surveillance efforts, the

---

[119] *See generally* Exec. Order No. 12,333, 3 C.F.R. 200, *reprinted in* 50 U.S.C. § 401 note (2000).

[120] *See generally* DoD Directive No. 5240.1, *supra* note 105.

[121] *See generally* USSID 18, *supra* note 13.

[122] *Id.*

[123] FISA, 50 U.S.C. § 1801(h)(1) (2000 & Supp. III 2003).

[124] *See* USSID 18, *supra* note 13, § 1.2.

[125] *See id.*

[126] *Id.* § 3.1.

[127] *Id.*

[128] *See id.*

agency may still retain, analyze, and disseminate such information under certain circumstances.[129]

Most of these specific situations are unknown because they seem to be enumerated in sections 4.4 to 4.7 of USSID 18, which have been redacted from the declassified version of the directive.[130] Some indications may be gleaned, however, from other declassified provisions.[131] For instance, USSID 18's definition of "foreign communication" provides some indication of the types of communications allowed to be retained.[132] Section 9.8 defines a foreign communication as "a communication that has at least one communicant outside the United States . . . ."[133] Although surveillance efforts directed at premises in the United States are not considered foreign communications under the definition, efforts aimed at foreign residences, which inadvertently result in the collection of calls to and from U.S. persons, clearly remain part of the definition.[134] The fact that these communications are considered "foreign communications" is significant because it is the stated policy of the NSA to "target or collect only foreign communications."[135] Because ECHELON and other NSA signals intelligence efforts are estimated to collect most foreign communications transmitted worldwide, the "inadvertent" surveillance of U.S. persons placing international telephone calls can be assumed to be quite frequent.[136]

In order to mitigate the effects of this unavoidable consequence of the NSA's foreign intelligence efforts, USSID 18 section 7.1 provides that "foreign intelligence information concerning U.S. persons must be disseminated in a manner which does not identify the U.S. person."[137] This is typically accomplished by redacting the U.S. person's name or by similar means.[138] USSID 18 does, however, allow dis-

---

[129] USSID 18, *supra* note 13, § 3.1.

[130] *See id.* §§ 4.4–4.7.

[131] *See id.* § 9.8.

[132] *See id.*

[133] *Id.* The definition also includes communications that are "entirely among foreign powers or between a foreign power and officials of a foreign power . . . ." *Id.*

[134] *See* USSID 18, *supra* note 13, § 9.8.

[135] *See id.* § 3.1.

[136] *See* Sloan, *supra* note 35, at 1474. ("It is alleged that ECHELON intercepts all major modes of signal transmission, including land-lines, high-frequency radio, microwave radio relay, communications satellites, subsea cables, and the Internet."); *see also* Loeb, *supra* note 42, at A3 (citing reports that estimate that the ECHELON system captures up to 3 billion communications each day).

[137] USSID 18, *supra* note 13, § 7.1.

[138] *Id.* ("Generic or general terms or phrases must be substituted for the identity (e.g. 'U.S. firm' for the specific name of a U.S. Corporation or 'U.S. Person' for the specific

semination of the U.S. person's identity in a number of circumstances.[139] For instance, section 7.2(c) allows a U.S. person's name to be disseminated if the person's identity is "necessary to understand the foreign intelligence information or assess its importance."[140] The section also includes a non-exhaustive list of situations that would satisfy this requirement.[141] For example, section 7.2(c) provides that inadvertently acquired information regarding a U.S. person may be disseminated directly to domestic law enforcement agencies if the information indicates that the U.S. person is somehow involved in criminal activity.[142] This can occur despite the fact that no warrant was issued to authorize the initial surveillance responsible for acquiring the incriminating evidence from the unsuspecting and otherwise constitutionally protected U.S. person.[143]

The Fourth Amendment has yet to be extended to prevent such a situation. The issue is difficult to resolve because those who have standing to challenge such surveillance are unaware that they were initially targeted for criminal investigation based on information gained through warrantless surveillance of their international phone calls by the NSA.[144] The current controversy involving the secret directive issued by President Bush may bring these issues before the Supreme Court in the near future. Should this occur, many key issues will be presented, and the next generation of Fourth Amendment rights may be defined.

---

name of a U.S. Person). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year . . . .").

[139] *Id.* § 7.2.

[140] *Id.* § 7.2(c).

[141] *Id.*

[142] USSID 18, *supra* note 13, § 7.2(c)(4). Information about a U.S. person can be kept and disseminated if "[t]he information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes." *Id.*

[143] *See id.*

[144] Although FISA requires the government to notify criminal defendants when it seeks to use, against the defendant, information obtained through electronic surveillance, this requirement is limited to information obtained pursuant to a FISA warrant and also does not apply unless the government seeks to introduce the evidence at trial. The statute does not require the government to inform the defendant about information used only to initiate a criminal investigation. If the government does not seek to introduce the FISA evidence at trial, then it presumably may keep that evidence secret. Moreover, this requirement also only applies in situations where FISA is applicable. Thus, lawfully warrantless non-FISA foreign surveillance is not subject to this limitation. *See* FISA, 50 U.S.C. § 1806(c)–(d) (2000 & Supp. III 2003).

Perhaps the controversy also will cause legal policymakers at the NSA to reexamine the application of the current minimization procedures expressed in USSID 18. If so, one question that the Court should consider, when determining whether to allow the dissemination of information without a warrant, is the degree to which those procedures should take into account the reasonableness of one's expectation of privacy. Because the scope of the Fourth Amendment's protection is based largely on the reasonableness of one's subjective expectation of privacy, it seems to follow that individuals should be able to take affirmative technological steps such as the use of encrypted Internet telephony that would provide them with heightened constitutional protection against unwarranted invasion.

III. Encrypted Voice over Internet Protocol, Cryptanalysis, and the Territorial Limits of Constitutional Rights

A. *Encrypted VoIP*

As technology advances, the ability of individuals to protect their privacy against undesired intrusion is growing. In recent years. an increasing number of people are using Internet telephony[145]—also known as Voice over Internet Protocol ("VoIP")—instead of traditional telephone services for their international telecommunications.[146] VoIP converts analog voice communications into a compressed digital data format that is then transferred from computer to computer over regular Internet protocol data networks.[147] This enables computer users to speak to one another via the Internet using their existing Internet connections, often at no additional cost.[148] Because the data is converted into a digital form prior to transmission, efforts are increasing to bring about widespread use of data encryption methods to protect these

---

[145] Elec. Privacy Info. Ctr., EPIC Internet Telephony Page, http://www.epic.org/privacv/voip (last visited Mar. 28, 2006) (defining and explaining Internet telephony).

[146] VoIP usage is on the rise, and major corporations are beginning to invest large sums in its development. In September 2005, eBay, Inc. purchased Skype Technologies, S.A. for $2.6 billion. Skype Technologies is currently the world leader in Internet telephony, with 54 million customers and projected revenue of more than $200 million in 2006. Although criticized by some as a risky investment by eBay, the move certainly demonstrates a strong expectation that use of Internet telephony will continue to grow significantly in coming years. *See* Jonathan Krim, *EBay's Skype Risk Is a Calculated One*, Wash. Post, Sept. 22, 2005, at D1.

[147] *See* Elec. Privacy Info. Ctr., *supra* note 145.

[148] *See id.*

communications from eavesdropping en route.[149] For instance, Skype Technologies, one of the world's leading VoIP providers, utilizes a 256-bit Advanced Encryption Standard ("AES") encryption algorithm that many experts believe to be functionally unbreakable.[150] Difficulties are posed, however, when users of one service attempt to communicate with users of another.[151]

Today, VoIP encryption is still in its infancy, with widespread inter-service usage being hindered by the difficulty in standardization of VoIP protocols and the unwillingness of some providers to offer open architectures that would allow different encryption algorithms to negotiate between communication endpoints.[152] These barriers are slowly being eroded by the efforts of privacy advocates and philanthropic cryptographic experts who are working to adapt popular open-source cryptosystems for widespread distribution and usage.[153] Thus, despite initial compatibility difficulties, the use of encrypted

---

[149] *See* Andreas M. Antonopoulos & Joseph D. Knape, *Security in Converged Networks*, INTERNET TELEPHONY, Aug. 2002, *available at* http://www.tmcnet.com/it/0802/0802gr.htm.

[150] *See* David S. Bennahum, *Can They Hear You Now?*, SLATE, Feb. 19, 2004, http://www.slate.com/id/2095777/ (quoting the National Institute of Science and Technology as stating that "it would take a computer using present-day technology 'approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key'"). Skype's 256-bit standard offers an even greater level of security. *Id.*

[151] Skype uses a proprietary protocol that is not compatible with many other standards, such as Session Initiation Protocol ("SIP") and Inter-Asterisk eXchange Protocol ("IAX"); therefore, users of other providers are often unable to communicate with users on the Skype network. *See* Brian Livingston, *Beware Skype's Hype; Focus on SIP-Compliant Internet Calling Instead*, EWEEK, Dec. 1, 2003, at 64 ("Skype isn't compatible with SIP. You could wake up one day to a nightmare in which some of your offices have adopted SIP while others have downloaded Skype. Users couldn't rely on the incompatible services to call one another."); *see also Skype's the Limit*, INFO. AGE, Sept. 21, 2005, http://www.information-age.com/article/2005/september/skypes_the_limit (discussing the prospect of adding VoIP service to Google Talk and stating that "Google favours using IP telephony technology from start up SIPphone, which is compatible with the Vonage service but not Skype.").

[152] *See* Antonopoulos & Knape, *supra* note 149; Livingston, *supra* note 151, at 64; *Skype's the Limit*, *supra* note 151.

[153] Most recently, the famous cryptographer Phillip Zimmermann announced a new encrypted VoIP program known as Zfone. In 1991, Zimmermann gained international acclaim from privacy advocates when he developed Pretty Good Privacy ("PGP"), an encryption program used to encrypt e-mail transmissions as well as stored data. Zimmermann distributed the software for free, even publishing the source code on the Internet, in order to allow peer scrutiny of the program. PGP was rumored to be unbreakable, even by the NSA, and Zimmerman subsequently became the target of an extensive three-year federal criminal investigation for alleged violations of U.S. export restrictions on dual-use cryptographic technology. *See* Ronald Bailey, *Code Blues*, REASON, May 1994, at 36; *see also* John E. Dunn, *Encryption Guru Returns with VoIP Software*, PCWORLD, July 27, 2005, http://www.pcworld.com/news/article/0,aid,122000,00.asp; Phil Zimmermann's Home Page, Background, http://www.philzimmermann.com/EN/background/index.html (last visited Mar. 28, 2006).

VoIP is beginning to spread and will soon become the standard for all voice-over-Internet communications.

Although VoIP communications originally could be freely captured and overheard by anyone possessing the requisite technical knowledge,[154] today's encrypted VoIP conversations are practically indecipherable, even by the most sophisticated professionals.[155] The NSA and CSS together form the world's premier cryptographic agency, employing the most advanced cryptanalytic capabilities in existence.[156] Through various means, the agency is able to decipher a significant percentage of the encrypted communications it captures each day via ECHELON and other means.[157] However, the decryption process involves additional steps that raise constitutional concerns.[158]

The decryption of encrypted VoIP communications requires the agency to take numerous additional steps in order to understand the information they have acquired.[159] Although ECHELON may cast a wide net, capturing most electronic communications transmitted worldwide, the NSA/CSS must employ extraordinary measures before any encrypted VoIP communication can be understood and analyzed.[160] This raises questions about the reasonable expectations of U.S. citizens employing these technologies and the extent to which the Constitution, through the application of the Fourth Amendment, should permit the government to use information gained through the frustration of those expectations.

---

[154] *See* Niall Magennis, *Skills Development*, Network News, Mar. 31, 1999 (available on LexisNexis) ("Security is critical to the future of VoIP because it is remarkably easy to listen in on current VoIP conversations using a protocol analyzer.").

[155] *See* Bennahum, *supra* note 150.

[156] Nat'l Sec. Agency/Cent. Sec. Serv., *supra* note 24.

[157] *See* Matthew Schwartz, *Intercepting Messages*, ComputerWorld, Aug. 28, 2000, at 48 (alleging that "Echelon is able to intercept and decrypt almost any electronic message sent anywhere in the world"). *But see* Sloan, *supra* note 35, at 1482–83 (discussing the limitations on the NSA's ability to decrypt communications encrypted using modern encryption programs).

[158] In Part IV of this Article, I argue that the government's use of the extraordinary measures necessary to crack encrypted VoIP violates the reasonable expectation of privacy held by protected persons under the Fourth Amendment. *See infra* notes 192–232 and accompanying text.

[159] *See* Max Schireson, *Decoding the Complexities of Cryptography*, PC Wk., Jan. 10, 1994, at 84 (discussing several methods of cryptanalysis).

[160] The term "extraordinary means" is used here to refer to the use of electronic or other resources which perform high-speed processing that exceeds the capabilities of human beings.

B. *Cracking Encrypted VoIP Through Cryptanalysis*

In order to provide a background for the cryptanalysis debate, it is helpful to define some of the basic terminology in the field. There is a distinct difference between decryption through cryptanalysis and through non-cryptanalytic means. The term "cryptanalysis" refers to methods through which encrypted messages are decrypted without having access to the password or passphrase that allows those messages to be deciphered.[161] In other words, this involves cracking the encryption itself.[162] In comparison, non-cryptanalytic methods involve learning or "stealing" the relevant passwords or passphrases.[163]

Cryptographers use many techniques to break codes directly. Although a detailed discussion of such cryptanalytic techniques is beyond the scope of this Article, it is useful to discuss briefly several cryptanalytic techniques in order to distinguish them from the more invasive non-cryptanalytic methods discussed in Part III.C. One form of cryptanalysis involves attacking the encryption algorithm directly. Because computer algorithms are used to encrypt data, structural weaknesses in those algorithms may be exploited to decipher messages encrypted using that method.[164] Many of the most popular encryption algorithms utilized today are open-source and have been tested extensively for the types of structural weaknesses that plagued some earlier encryption standards.[165] Although the structural integ-

---

[161] BBC.co.uk, Basic Cryptanalysis, http://www.bbc.co.uk/dna/h2g2/alabaster/A613135 (last visited Apr. 5, 2006).

[162] *See id.*

[163] *See id.*

[164] An algorithm is a set of instructions which is performed to accomplish a certain task. In the case of encryption software, the encryption algorithm performs a set of recurring operations to scramble data into an unintelligible form. Because of the recurring nature of these operations, a weakness in the design of the algorithm can produce patterns which can be exploited to decrypt data which has been encrypted using that method. *See* Scott Fluhrer, Itsik Mantin, & Adi Shamir, Weaknesses in the Key Scheduling Algorithm of RC4 (unpublished manuscript), *available at* http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf (last visited Mar. 30, 2006) (exposing a major flaw in Wired Equivalent Privacy ("WEP") that stemmed from the fact that its key scheduling algorithm caused the same keys to be repeated often and at predictable intervals); *see also* Rik Farrow, *Wireless Security: Send in the Clowns?*, NETWORK MAG., Sept. 1, 2003, at 54 (discussing WEP's vulnerability); Bob Walder, *Networks Focus; Cryptography*, COMPUTER WKLY., Nov. 25, 2003, at 50 (providing an explanation of public and private key encryption systems).

[165] Open-source programs are assumed to be well-tested because anyone in the world is free to examine them; however, some experts caution that open-source availability does not necessarily guarantee security. *See* Gary McGraw & John Viega, *Practice Safe Software Coding*, INFO. SECURITY, Sept. 2001, at 62 ("One common fallacy is to believe that open-source software is likely to be secure, because its availability will lead to people performing

rity of such algorithms is sound, their open-source nature means that there is no secret as to their operation.[166] Therefore, the only thing standing in the way of sophisticated decryption efforts is the strength of the key that controls the operation of the cipher.[167]

Cryptographers use many methods to decipher encryption keys. For example, encrypted texts may be subjected to a number of techniques, such as "brute force" attack,[168] differential cryptanalysis,[169] or known-plaintext and chosen-plaintext attacks.[170] All are means of deciphering messages without having access to the passphrase used to decode them. In theory, virtually all ciphers can be broken by "brute force" or other cryptanalytic means.[171] However, given the myriad of possible keys and passphrases that could be used, these methods often prove to be too time consuming for practical application.[172] For example, the National Institute of Science and Technology estimates that it would take a standard computer approximately 149 trillion years to break even a 128-bit AES key, which is currently half the length of the AES keys used to encrypt Skype's VoIP transmissions.[173]

Even assuming the vastly superior computational abilities of the NSA, standard decryption via conventional cryptanalytic means would be very inefficient.[174] Although the specific methods of the NSA are

---

security audits. . . . There [is] strong evidence to suggest that source code availability does [not] provide strong incentive for people to review the code design.").

[166] Kerckhoffs' Law stands for the proposition that, regardless of the sophistication of the data encryption algorithm, one should never rely on the secrecy of the algorithm alone to maintain the security of encrypted data. Because of the nature of algorithms, it is reasonable to assume that the details of the algorithm's operation are known to whomever is attempting to decrypt encrypted ciphertext. Security is provided not by the secrecy and complexity of the algorithm, but rather by the secrecy and complexity of the key. *See* BBC.co.uk, *supra* note 161.

[167] *See id.*

[168] The simplest form of cryptanalysis is known as a "brute force attack." This method involves bombarding an encrypted message with every possible key or passphrase in an attempt to decipher the code. *Data Encryption Essentials; Software Security*, Software World, Sept. 1, 2005, at 15.

[169] *See* Max Schireson, *Decoding the Complexities of Cryptography*, PC Wk., Jan. 10, 1994, at 84 (providing a description of differential cryptanalysis).

[170] *See* George T. Friedlob et al., *An Auditor's Primer on Encryption*, CPA J., Nov. 1, 1997, at 40 (describing known-plaintext and chosen-plaintext attacks). *See generally* Howard M. Heys. *A Tutorial on Linear and Differential Cryptanalysis*, 26 Cryptologia 189 (2002).

[171] *See* Peter Coffee, *No Crypto Is Too Tough to Crack*, PC Wk., Sept. 29, 1997, at 16.

[172] *See* Bennahum, *supra* note 150 (discussing the incredible amount of time necessary to perform a successful brute force attack on a message encrypted using 128-bit AES encryption).

[173] *See id.*

[174] *See id.*

not publicly known, it can be assumed that the agency uses such methods only as a last resort. Direct cryptanalysis is unnecessary if the NSA is able to determine a person's passphrase. This could be achieved though a variety of means. In addition to the more forceful "rubber-hose" methods,[175] there are a number of non-cryptanalytic techniques that the NSA could employ to learn a suspect's passphrase.

C. *Non-Cryptanalytic Means of Cracking Encrypted VoIP*

Given the difficulty of applying direct cryptanalytic methods to defeat the use of modern encryption programs, the U.S. government has developed other means of deciphering these conversations.[176] Such non-cryptanalytic methods include social engineering,[177] signals intelligence (electronic surveillance). phishing,[178] site spoofing (pharming),[179] and keystroke logging.[180] In late 2001, the Federal Bureau of Investigation (the "FBI") was reported to have developed its own key-

---

[175] The term "rubber-hose cryptanalysis" refers to the use of torture or other coercive means to obtain keys and passphrases from those in possession of them. *See* Tech FAQ, What Is Rubber Hose Cryptology?, http://www.tech-faq.com/rubber-hose-cryptology.shtml (last visited Apr. 7, 2006); *see also* Danny O'Brien, *Yahoo Has Power to End Chinese Net Censorship*, IRISH TIMES, Sept. 30, 2005, at 7 (discussing the use of rubber-hose cryptanalysis in China).

[176] *See* Elizabeth Clark, *Illuminating Magic Lantern*, NETWORK MAG., Feb. 1, 2002, at 18 (discussing the FBI's keystroke-logging Trojan Horse virus known as "Magic Lantern").

[177] Social engineering is a broad term that encompasses many other forms of non-cryptanalytic tactics such as phishing and pharming. Social engineering involves exploiting the naiveté of unsophisticated computer users to gain knowledge of passphrases and other personal data. *See Security Dictionary*, INFO. AGE, May 11, 2005, *available at* http://www.information-age.com/article/2005/may/security_dictionary.

[178] Phishing is a tactic often used by hackers whereby an e-mail is sent to various users claiming to be from a well-known financial organization. Such e-mails often claim that a problem has arisen that requires the recipient to log in to a website purportedly administered by the financial organization. When the person logs into the fake site, he or she ends up providing his or her password and login details to criminals who then use the information to gain access to the user's actual account. *See* Chris Green, *Data Business; 'Tis the Season to Beware Phishing Scams*, COMPUTING, Dec. 15, 2005, at 38.

[179] Site spoofing, also known as "pharming," is often performed in conjunction with phishing. Site spoofing involves manipulation of the Domain Name System to direct Internet traffic to imposter websites. These imposter sites appear to be the exact same as the legitimate company being spoofed. When customers attempt to log in to these sites their user IDs, passwords, credit card numbers, or other personal data is sent directly to the criminals running the site. *See* Catherine Sanders Reach, *Pharming & Other New Hacker Scams*, L. TECH. NEWS, May 2005, at 46 (offering an explanation of "pharming").

[180] *See* Susanna Schrobsdorff, *Cyber-Insecurity*, NEWSWEEK (web exclusive), June 21, 2005, http://www.msnbc.msn.com/id/8306655/site/newsweek.

stroke-logging virus.[181] The program, known as "Magic Lantern," works like the standard keystroke-logging Trojan horse viruses traditionally used by hackers.[182] The FBI surreptitiously uploads its keystroke-logging software onto the computers of those it seeks to surveil.[183] Once installed, this program allows the FBI to record every keystroke that users type into the infected computer.[184] When the suspect types in his or her passphrase, this information is captured and then may be used to decipher every communication or file that is encrypted using the same phrase.[185]

Although the FBI must obtain a warrant in order to install such programs on computers within the United States, the NSA is not required to obtain a warrant before installing similar programs on the computers of non-U.S. persons abroad.[186] As a result, U.S. persons contacting foreign persons abroad via e-mail or Internet telephony may have those communications compromised despite the use of encryption.

D. *U.S. Legal Restraints on the Use of Cryptanalytic and Non-Cryptanalytic Tactics on Non-U.S. Persons Outside the United States*

Under U.S. law, there are virtually no legal restraints on the ability of the NSA to use cryptanalytic or non-cryptanalytic tactics against non-U.S. persons outside the United States.[187] It has long been recognized that the U.S. Constitution does not extend its protections outside U.S. borders, except with respect to U.S. persons.[188] For example, in 1990, in *United States v. Verdugo-Urquidez*, the Supreme Court held that the Fourth Amendment does not place any limits on the ability of U.S. government agents to perform even physical searches of the homes of aliens outside the United States.[189] A natural extension of this decision is that no warrant is required for even the most intrusive

---

[181] Dan Verton, *Feds Boost Online Surveillance Activity*, CNN.COM, Dec. 11, 2001, http://archives.cnn.com/2001/TECH/internet/12/11/online.surveillance.idg/index.html.

[182] Christopher Woo & Mirada So, *The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance*, 15 HARV. J.L. & TECH. 521, 524 (2002).

[183] *See id.*

[184] Neal Hartzog, Comment, *The "Magic Lantern" Revealed: A Report of the FBI's New "Key Logging" Trojan and Analysis of Its Possible Treatment in a Dynamic Legal Landscape*, 20 J. MARSHALL J. COMPUTER & INFO. L. 287, 288 (2002).

[185] *See id.*

[186] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990).

[187] *See supra* notes 51–144 and accompanying text.

[188] United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 318 (1936).

[189] 494 U.S. at 274–75.

electronic invasions of foreign computers by government agents.[190] In light of the length of time it takes to perform actual cryptanalysis to break ciphers and the lack of legal restrictions in this area, it can be assumed that the NSA widely employs methods similar to Magic Lantern and has installed Trojan horse software on many computers of interest throughout the world.

Given the NSA's exceptional cryptanalytic resources and the absence of domestic legal restraints on the agency's use of non-cryptanalytic methods on aliens outside the United States, even the most private international VoIP calls of U.S. citizens probably may be overheard, despite the use of reasonable steps to maintain privacy. Even American citizens who have taken every reasonable precaution to avoid eavesdropping—by using encrypted VoIP technology—may have their conversations decrypted and overheard by the NSA as a result of the use of invasive non-cryptanalytic techniques against the NSA's foreign contact. This is although the use of such techniques clearly would be illegal if conducted directly against the U.S. person without a warrant.[191] Situations such as this violate the reasonable expectations of American citizens who use encrypted VoIP technology. When information acquired through these means is then used by the government to initiate a criminal investigation against a U.S. person, a court should find that the Fourth Amendment has been violated.

IV. The Constitutional Overbreadth of USSID 18 § 7.2(c)(4) as Applied to the Encrypted VoIP Conversations of U.S. Persons

A. *The Fourth Amendment and Reasonable Expectations of Privacy*

The Fourth Amendment places its protections largely in the hands of individuals. It guarantees that protected persons will not be subjected to warrantless government invasions of their private lives if they take reasonable measures to ensure their privacy.[192] The warrant requirement of the Fourth Amendment extends to situations where an objectively reasonable and legitimate expectation of privacy ex-

---

[190] *See id.*

[191] The Fourth Amendment requires the government to obtain a warrant before using invasive methods of cryptanalysis in most cases. *See* United States v. Scarfo, 180 F. Supp. 2d 572, 577–78 (D.N.J. 2001) (explaining that the FBI needed a warrant to install a keystroke-logging program on a suspect's computer).

[192] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

ists.[193] Although one is not entitled to claim privilege over matters left open to the world, people may expect that private conversations will remain free from unwarranted government surveillance if reasonable measures have been taken to keep those conversations from being overheard.[194] If such measures have been taken, then a reasonable expectation of privacy exists, and those conversations may not be surveilled absent probable cause and a warrant demonstrating that proof has been made to that effect.[195]

The Supreme Court has established a two-part analysis that is used to determine whether a particular area is entitled to Fourth Amendment protection.[196] First, the person must have "manifested a subjective expectation of privacy" in that area.[197] It would be difficult to argue that this prong is not satisfied in the case of either encrypted or unencrypted VoIP because it can be assumed that most people hold a subjective expectation that their private telephonic conversations will not be overheard by unknown third parties. This subjective expectation is manifested even more clearly when users choose to protect their conversations through encryption.

Second, the expectation of privacy must be one that "society is willing to recognize as legitimate."[198] The Supreme Court has generally adopted a rights-based approach to handling this second criterion, finding that one must have a right of privacy in the disputed area enforceable outside of the Fourth Amendment to claim a legally justifiable expectation of privacy.[199] Society has long recognized the

---

[193] *See* California v. Ciraolo, 476 U.S. 207, 211 (1985).

[194] *See Katz*, 389 U.S. at 352 (holding that even a telephone conversation taking place in a public telephone booth is entitled to Fourth Amendment protection, provided that the individual closes the door).

[195] *See id.* at 357 ("'Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes,' and that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment . . . .") (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951)) (footnote omitted).

[196] *Id.* at 361 (Harlan, J., concurring); *see also* Bond v. United States, 529 U.S. 334, 338 (2000) ("Our Fourth Amendment analysis embraces two questions. First, we ask whether the individual, by his conduct, has exhibited an actual expectation of privacy; that is, whether he has shown that 'he [sought] to preserve [something] as private. . . .' Second, we inquire whether the individual's expectation of privacy is 'one that society is prepared to recognize as reasonable.'") (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)) (footnote omitted).

[197] *Ciraolo*, 476 U.S. at 211.

[198] *Id.*; *see also Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[199] *See* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy"?*, 33 CONN. L. REV. 503, 508 (2001).

legitimacy of one's expectation of privacy during telecommunications. For example, both FISA and the ECPA make it a felony to engage in nonconsensual telephonic eavesdropping without a warrant.[200] VoIP is essentially a telephone call that is made using alternative means. Accordingly, it is illogical to argue that society would be willing to accept phone conversations as legitimately private when conducted via traditional phone networks but somehow illegitimate and unprotected when conducted via secure Internet telephony.[201] Thus, both prongs of the test are satisfied. Accordingly, VoIP conversations should be protected by the Fourth Amendment, and the government should be required to obtain a warrant prior to undertaking targeted surveillance of such conversations.[202]

---

[200] *See* FISA, 50 U.S.C. § 1809 (2000); *see also* ECPA, 18 U.S.C. § 2511 (2000 & Supp. III 2003).

[201] Initially, courts had been unwilling to recognize a reasonable expectation of privacy in calls made using cordless telephones due to the ease with which they could be inadvertently monitored. *See* McKamey v. Roach, 55 F.3d 1236, 1239–40 (6th Cir. 1995). In 1994, Congress passed the Communications Assistance for Law Enforcement Act, which extended the wiretapping prohibitions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, making them applicable to eavesdropping on cordless telephones as well as land-based phones. Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, § 202, 108 Stat. 4279, 4290–91 (1994) (codified at 18 U.S.C. §§ 2510–2511 (2000 & Supp. III 2003)). Even before Congress extended Title III's protections, the situation posed by portable phones was entirely distinguishable from the case of both traditional and encrypted VoIP. Although neighbors using similar phones could inadvertently overhear cordless telephone calls, eavesdropping on traditional VoIP conversations requires intentional efforts by someone with an uncommon level of computer knowledge and skill. In the case of encrypted VoIP, not only are such conversations immune from casual or inadvertent eavesdropping, but intentional surveillance also is rendered ineffective by the level of encryption employed. Only the most sophisticated technicians with access to state-of-the-art equipment and extraordinary computational resources would be able to decrypt such communications. Thus, due to the almost unparalleled security of VoIP communications, the Fourth Amendment certainly should extend to protect users' expectations that their encrypted VoIP conversations will not be surveilled by the government without a warrant.

[202] Although courts generally have refused to recognize a general right to privacy for web surfing and other public activities on the Internet, the issue of whether the government may seize private person-to-person Internet communications en route is a different matter entirely. *See* Mitchell Waldman, Annotation, *Expectation of Privacy in Internet Communications*, 92 A.L.R. 5TH 15, § 5 (2001). Courts have already recognized a person's reasonable expectation that private e-mails and phone conversations will not be intercepted by the government en route without a warrant. *E.g.*, United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) ("The transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant.") (citing United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996)); United States v. Long, 61 M.J. 539, 546 (N-M. Ct. Crim. App. 2005) ("[W]hile the e-mails may have been monitored for purposes of maintaining and protecting the system from malfunction or abuse, they were subject to seizure by law enforcement personnel only by disclosure as a

Although it is clear that U.S. persons are protected from warrantless government surveillance targeting their VoIP conversations, U.S. persons are not currently protected from situations where such conversations are surveilled indirectly by the government during the otherwise lawful warrantless surveillance of non-U.S. persons abroad. When such a situation occurs, and information to and from U.S. persons is collected without a warrant, the Fourth Amendment should still apply, and the reasonable expectations of protected persons should be respected.

B. *Are Some Expectations More Reasonable than Others?*

Arguably, a U.S. citizen's expectation of privacy in international communications has never been more reasonable. According to estimates, it would take a computer trillions of years to decipher a message encrypted using an encryption standard that employs a key length half of that currently used by Skype.[203] Consequently, encrypted VoIP users can be certain not only that their communications are virtually immune from random eavesdropping, but that even the NSA would find it difficult—perhaps even impossible—to surveil those conversations purposefully, even with the extraordinary computational resources at their disposal.[204] Because encrypted VoIP is so secure, it stands to reason that one's expectation of privacy in such communications is much higher than it is with almost any other form of communication. Because Fourth Amendment protection is based largely on the reasonableness of one's expectations, it would seem that using encrypted VoIP should provide U.S. citizens with the highest level of Fourth Amendment protection.[205]

Some scholars disagree with this assessment, contending instead that the use of encryption can never provide a reasonable expectation

---

result of monitoring or when a search was conducted in accordance with the principles enunciated in the 4th Amendment."). Moreover, this recognition has come despite the susceptibility of e-mails to eavesdropping by hackers. *See* Ed Oswald, *Gmail Bug Exposes E-mails to Hackers*, BETANEWS, Jan. 12, 2005, http://www.betanews.com/article/Gmail_Bug_Exposes_Emails_to_Hackers/1105561408. Although direct application of these principles to Internet telephony remains scarce, presumably—given its similarity to e-mail messages as discussed in *United States v. Monroe*—traditional VoIP will be afforded equivalent constitutional protection in the future. *See id.*; *see also Monroe*, 52 M.J. at 330.

[203] *See* Bennahum, *supra* note 150.

[204] *See id.*

[205] *See* Sean J. Edgett, Comment, *Double-Clicking on Fourth Amendment Protection: Encryption Creates a Reasonable Expectation of Privacy*, 30 PEPP. L. REV. 339, 365 (2003) (arguing that the use of encryption creates a reasonable expectation of privacy).

of privacy.[206] In a 2001 article, Professor Orin Kerr argues that encryption can never offer a reasonable expectation of privacy for Fourth Amendment purposes because the Fourth Amendment limits only the acquisition of materials, not the process used to analyze the materials already in the government's possession.[207] This argument presupposes that information in the hands of the government has always come into its possession pursuant to some sort of warrant, plain view, or other constitutionally permissible means. It fails to consider the situation posed by the lawful warrantless surveillance conducted daily by U.S. intelligence agencies on foreign persons abroad. Lawful international signals intelligence operations result in an enormous amount of data coming into the possession of the government without a warrant each day.[208] Under Professor Kerr's analysis, which finds that encryption itself offers no reasonable expectation of privacy, the government would be free to do what it pleases with the data collected even if it was obtained through warrantless surveillance of U.S. citizens.[209] Once the data was lawfully in the possession of the government, the Fourth Amendment's protections could never be triggered.

This argument is untenable in light of the Supreme Court's Fourth Amendment jurisprudence. The issue of whether an item is constitutionally protected is determined based solely on whether the person claiming protection had manifested a subjective expectation of privacy in that item, and whether that expectation is one which society is willing to recognize as reasonable.[210] It is the reasonableness of one's expectations that controls, not the location of the challenged evidence.[211] The fact that a piece of evidence is already in the hands of the government is irrelevant to the constitutional analysis and simply begs the question.

---

[206] *See* Kerr, *supra* note 199, at 532.

[207] *See id.* at 505 ("[E]ncryption cannot create Fourth Amendment protection because the Fourth Amendment regulates government *access* to communications, not the *cognitive understanding* of communications already obtained.").

[208] *See* Loeb, *supra* note 42, at A3.

[209] Professor Kerr's argument sets up an artificial all-or-nothing scenario. Under his view, either all encryption creates a reasonable expectation of privacy, or no encryption creates such an expectation. *See* Kerr, *supra* note 199, at 524 ("[I]f encryption can 'lock' a communication and create a reasonable expectation of privacy, then *every kind* of encryption, ranging from Pig Latin . . . to the strongest public key encryption, must trigger the same Fourth Amendment protection.").

[210] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[211] *See id.* at 352 (majority opinion).

Professor Kerr's analysis uses a plain-view rationale to explain why review of items already in the possession of the government should not be subject to any further Fourth Amendment limitations.[212] This argument, however, ignores the fact that just because an item may be readily seen by the government does not necessarily mean that the item is in plain view.[213] The simple fact that a piece of encrypted ciphertext may be seen by police does not mean that its contents are readily visible. In order to truly see the underlying message, government agents must employ tactics and resources beyond mere human analysis in order to bring the decrypted message's contents into view. When encrypted data has come into the possession of the government without a warrant, and in violation of the reasonable expectations of a protected person, the decryption of that data should require a warrant.

The Supreme Court's jurisprudence in this area makes it clear that the "plain view" doctrine requires materials seized in warrantless searches to have been readily visible to the naked eye without the use of extraordinary or superhuman means.[214] In 2001, in *Kyllo v. United States*,

---

[212] *See generally* Kerr, *supra* note 199. To support his claim that the Fourth Amendment does not limit the efforts of law enforcement once materials are already in their possession, Professor Kerr offers an oversimplification of the decryption process likening it to taping together torn papers, solving riddles, understanding Pig Latin, or reading a doctor's messy handwriting. *See id.* at 520, 521, 524. To be sure, the examples offered by Professor Kerr would not be entitled to protection; however, this is not because the "encrypted" items are in the hands of the government, but rather because they may be interpreted through human effort and are therefore in plain view. Torn papers may be taped together, foreign languages may be interpreted, and messy handwriting may be readily understood without technological assistance. Cryptanalysis of computer-generated encryption, however, requires the use of advanced computational resources that vastly surpass human capacity.

[213] Professor Kerr compares encrypted ciphertext to a riddle and points out that, regardless of the difficulty of a particular riddle, one could never expect a Fourth Amendment expectation of privacy with respect to its meaning. *Id.* at 522–24. Again, this analogy fails to recognize the difference between what can be seen or decrypted using human effort and what can be seen only by using extraordinary means beyond natural human capacitv. *See id.* at 522.

[214] *See* Florida v. Riley, 488 U.S. 445, 450–51 (1989) (holding that a defendant did not have a reasonable expectation of privacy in a greenhouse, the contents of which were clearly visible from the sky). In *Florida v. Riley*, where police peered inside the defendant's greenhouse from a helicopter hovering 400 feet above the greenhouse, the Court discussed the altitude of the police helicopter at length, and the fact that the greenhouse's contents were visible with the naked eye was crucial to the Court's finding that the area was not protected by the Fourth Amendment. *See id.* at 450. Likewise, the police in *California v. Ciraolo* used a small plane to hover 1000 feet above the defendant's backyard; had they needed special X-ray goggles or the use of a supercomputer to view the marijuana plants growing in the backyard, presumably the Court would have found that such efforts re-

the Court specifically rejected the argument that high technology could be used to view the contents of protected areas not readily seen by the naked eye.[215] The *Kyllo* Court noted that a contrary approach would leave the Fourth Amendment's protection "at the mercy of advancing technology."[216] Specifically, the Court ruled in *Kyllo* that the government may not use thermal imaging technology to learn about the contents of a protected space without a warrant.[217] A natural extension of this holding is that the government is also prohibited from using technology to learn about the contents of a protected communication without a warrant.[218]

This is not to say that the government may not use computers to decrypt data that is already in its possession pursuant to a lawfully issued warrant. The Fourth Amendment does not stand for the proposition that a person's reasonable expectation of privacy will *never* be violated by the government, only that a warrant is required to do so.[219] Such information may be decrypted not because it is already in the possession of the government—as asserted by Professor Kerr—but rather because it has come to be in its possession pursuant to a warrant issued after a showing of probable cause. In instances where conversations have come into the possession of the government without a war-

---

quired a warrant. *See Ciraolo*, 476 U.S. at 215 ("[I]t is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.").

[215] 533 U.S. 27, 34–35 (2001).

[216] *Id.* at 35. *See generally* Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325 (2002) (discussing the constitutional restraints on the government's ability to use technology to enhance surveillance capabilities).

[217] *Kyllo*, 533 U.S. at 40.

[218] Professor Kerr offers a hypothetical involving a terrorist named Lex Luthor who places an ad in a newspaper containing an obvious and easily broken code detailing a plot to blow up a New York City subway station. *See* Kerr, *supra* note 199, at 519. If one simply rips up a piece of paper or utilizes a simple encryption standard that can be broken through basic human effort, such as the simple substitution cipher referenced in Professor Kerr's Lex Luthor hypothetical, then not even the fiercest privacy advocate would argue that a reasonable expectation of privacy exists. *See* Kerr, *supra* note 199, at 519. To be sure, no one could reasonably claim an expectation of privacy in a newspaper advertisement. However, if a U.S. citizen is communicating with a friend telephonically—an area long recognized by society as legitimately private—and that person utilizes a military-grade encryption standard, thus rendering their conversations indecipherable to all but the NSA, then that person is entitled to Fourth Amendment protection because the expectation of privacy is reasonable. The fact that the government is already in possession of the encrypted information is irrelevant to the inquiry.

[219] *See* U.S. CONST. amend. IV.

rant, the reasonable expectations of the person surveilled must be respected.

To be sure, the government should not be required to determine a person's protected status prior to all signals collection efforts. Such an assessment would be impossible in the case of inadvertently acquired information. A person's reasonable expectations should simply be respected to the fullest extent practicable, and information collected from a U.S. person without a warrant should never be used to initiate general domestic criminal investigations against them unless truly exigent circumstances are presented.

Professor Kerr states that "the Fourth Amendment is not a roving privacy machine," but in many ways, it is.[220] The Supreme Court has long held that "the Fourth Amendment protects people, not places."[221] This protection travels with a person wherever he or she goes, and it covers all situations where a legitimate expectation of privacy can be held.[222] The Supreme Court has made it clear that it is the reasonableness of a person's expectation of privacy, not the geographic location of the conversation in question, that determines whether or not a conversation is protected.[223] American citizens do not lose their Fourth Amendment rights simply because they set foot outside the United States; likewise, their conversations do not become fair game once the electrons transmitting them pass beyond U.S. borders.[224]

---

[220] *See* Kerr, *supra* note 199, at 506.

[221] *Katz*, 389 U.S. at 351.

[222] The Supreme Court has rejected the argument that an individual's Fourth Amendment protection is limited to certain physical locations. Instead, according to the Court, the protection travels with the individual, and even phone calls made from public telephones may be protected if they are conducted in a manner that prevents them from being casually overheard. *See id.* at 352.

[223] *See id.*

[224] Although the Supreme Court has never had occasion to hold that the Fourth Amendment extends to protect American citizens from the acts of U.S. agents abroad, it seems likely that the Court would do so if the issue were ever brought before it. *See generally* United States v. Conroy, 589 F.2d 1258, 1264 (5th Cir. 1979) ("The Fourth Amendment not only protects all within our bounds; it also shelters our citizens wherever they may be in the world from unreasonable searches by our own government."). The Circuit Courts of Appeals are almost unanimous on the issue, as demonstrated by their application of the joint venture doctrine. The joint venture doctrine states that the Fourth Amendment does not apply to searches conducted against U.S. persons abroad unless the searches are performed by U.S. agents or by foreign agents who are acting in close association with U.S. agents. *See* United States v. Morrow, 537 F.2d 120, 139 (5th Cir. 1976) (stating that the exclusionary rule may be invoked if U.S. agents are involved in an unlawful search conducted by foreign officials overseas); *see also* United States v. Behety, 32 F.3d 503, 510 (11th Cir. 1994) (stating that the Fourth Amendment may apply to a foreign search "if the foreign officials conducting the search were actually acting as agents for their American

C. *Redrafting USSID 18 § 7.2(c)(4) to Respect Reasonable Expectations of Privacy*

The reasonable expectation of privacy held by those using encrypted VoIP should afford them the highest level of protection available under the Fourth Amendment. Although such Fourth Amendment protection should not prevent the government from analyzing inadvertently acquired information, it should certainly prevent it from using such information against protected persons except in cases of emergency or situations where serious national security concerns are involved.

Under most circumstances, USSID 18 minimizes the impact of NSA surveillance on U.S. persons.[225] Under the directive, when information pertaining to a U.S. person is inadvertently acquired, either it must be destroyed or the U.S. person's identity must be obscured or redacted from all reports.[226] However, USSID 18 section 7.2(c)(4) allows information obtained without a warrant to be kept and disseminated to law enforcement if it evinces any criminal conduct on the part of the inadvertently surveilled U.S. person.[227] No consideration is

---

counterparts"); United States v. Mount, 757 F.2d 1315, 1318 (D.C. Cir. 1985) (stating that the "exclusionary rule does apply to a foreign search if American officials or officers participated in some significant way"); Stonehill v. United States, 405 F.2d 738, 743 (9th Cir. 1968) (stating "the Fourth Amendment could apply to raids by foreign officials only if Federal agents so substantially participated in the raids so as to convert them into joint ventures between the United States and the foreign officials"). In addition, the Supreme Court has clearly extended other Bill of Rights protections to cover U.S. citizens abroad, which makes it highly unlikely the Court would refuse to do so with respect to the Fourth Amendment. *See* Reid v. Covert, 354 U.S. 1, 7–9 (1957) (extending Fifth and Sixth Amendment protection to American citizens abroad, and holding that "constitutional protections for the individual were designed to restrict the United States Government when it acts outside of this country, as well as here at home").

[225] *See generally* USSID 18, *supra* note 13.

[226] *Id.* § 7.1 ("Except as provided in Section 7.2, foreign intelligence information concerning U.S. persons must be disseminated in a manner which does not identify the U.S. persons. Generic or general terms or phrases must be substituted for the identity . . . ."); *see also* NAT'L SEC. AGENCY / CENT. SEC. SERV., U.S. IDENTITIES IN SIGINT (1994), at app. A, p. 2, *available at* http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB24/nsa11d.pdf (declassified version with some language redacted by the NSA) ("Unless specific approval has been granted to identify a U.S. [text redacted] or organization, reporters must use a generic identification. Reporters must also be careful not to use any information that allows a reader to identify the person or organization by context."); *id.* at 28 ("End the inadvertent intercept of communications solely between U.S. persons upon recognition of that fact. [text redacted] When such material is retained, do not retain any personally identifiable information (other than equipment names and technical data) concerning U.S. persons.").

[227] USSID 18, *supra* note 13, § 7.2(c)(4).

given to the reasonableness of the communicant's expectation of privacy, and no limitations are expressed regarding the types of offenses that may be revealed.[228]

Under the provision as it is currently written, evidence that an American citizen may have committed a misdemeanor could properly be disseminated to police for local criminal investigation.[229] There is no differentiation or qualification regarding the seriousness of the offense revealed.[230] Without any limitation on the type of "criminal" information that can be turned over to law enforcement, this provision represents a violation of the Fourth Amendment rights of those surveilled.[231] A reasonable limitation must be placed on this dissemination power, limiting it to situations where grave national security or other emergency situations are presented. Most of the other exceptions listed under USSID 18 section 7.2(c) require some form of exigent circumstance to exist before a U.S. citizen's identity may be divulged.[232] Section 7.2(c)(4) likewise should contain such limits.

Conclusion

Although the NSA's surveillance capabilities have grown considerably in recent years, so have the means through which citizens may affirmatively protect their own privacy. New forms of encrypted Internet telephony are offering Americans the ability to provide unparalleled security for their international telecommunications. Such methods were not generally available to the public when the current version

---

[228] *See id.*

[229] *See id.*

[230] *See id.*

[231] *See id.*

[232] *See* USSID 18, *supra* note 13, § 7.2(c). All but two of the exceptions listed under USSID 18 section 7.2(c) require the existence of circumstances which raise serious national security or public safety concerns. Subsection 1 provides an exception if the information indicates that the U.S. person may be an agent of a foreign power. *Id.* § 7.2(c)(1). Subsection 2 allows disclosure if it appears the U.S. person may be "engaged in the unauthorized disclosure of classified information." *Id.* § 7.2(c)(2). Subsection 3 allows disclosure if the U.S. person is involved in international drug trafficking. *Id.* § 7.2(c)(3). Subsection 5 allows disclosure if the information indicates that a "U.S. person may be the target of hostile intelligence activities of a foreign power." *Id.* § 7.2(c)(5). Subsection 6 allows disclosure if the information is pertinent to a threat to the safety of an organization or person. *Id.* § 7.2(c)(6). The only two exceptions listed under USSID 18 section 7.2 that do not raise potentially serious consequences for non-disclosure are: (1) subsection 7, which allows disclosure of the identities of senior executive branch officials; and (2) subsection 4, which allows disclosure of information that indicates any act of criminal behavior, with no limitation on the type or seriousness of the criminal conduct that may trigger the exception. *See id.* § 7.2(c)(4), (7).

of USSID 18 was drafted in 1993. Even before the advent of encrypted VoIP, courts had recognized that U.S. citizens held a reasonable expectation that their e-mails and communications would not be captured en route by the government without a warrant.[233] Now that encryption technology is becoming more widely available, U.S. citizens are enjoying an extraordinary expectation of privacy, the reasonableness of which is unprecedented in the field of communication.

The NSA is perhaps the most important force protecting the United States from foreign terrorism and other threats to national security. The information provided by the agency informs national security and foreign policy decisionmakers, thereby also playing a vital role in ensuring international peace and security. While the incredible value of this agency cannot be overstated, neither can the risks posed by its vast capabilities. The broad scope of the agency's vigilant efforts has the potential to threaten the legitimate rights of American citizens, and appropriate checks must be in place.[234]

FISA provides a well-established legal framework that has protected the rights of American citizens from unwarranted government surveillance since 1978.[235] Although it appears that this framework recently may have been circumvented through a secret executive order,[236] warrantless surveillance of Americans is nothing new.[237] Gaps in our legal protections have existed since FISA's enactment.[238]

The NSA's minimization procedures provide strong protection for the rights of U.S. citizens under most circumstances, but they allow breaches to occur in situations that are arguably the most crucial. Although the NSA is required to destroy information inadvertently obtained about U.S. citizens in most cases, the current minimization procedures allow the agency effectively to initiate criminal investigations by turning over such information to law enforcement if criminal conduct is revealed. This places Americans at risk of criminal prosecution resulting from warrantless eavesdropping on their private telecommunications. This should not be permitted. Although it may not be practicable for the NSA to obtain a warrant in every case where

---

[233] *See* United States v. Jones, 149 F. App'x 954, 959 (11th Cir. 2005); *see also* United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000).

[234] *See* Olmstead v. United States, 277 U.S. 438, 472–73 (1928) (Brandeis, J., dissenting) (providing a more fervent expression of this concept).

[235] *See* FISA, 18 U.S.C.A. §§ 2511, 2518, 2519, 50 U.S.C.A. §§ 1801–1811, 1821–1829, 1841–1846, 1861–1862, 1871 (West 2001 & Supp. 2005).

[236] *See* Risen & Lichtblau, *supra* note 2, at A1.

[237] *See supra* notes 51–144 and accompanying text.

[238] *See supra* notes 51–144 and accompanying text.

information about U.S. citizens may be inadvertently acquired, the heightened expectation of privacy provided by encrypted Internet telephony should require additional limitations on what may be done with such information after it is acquired.

USSID 18 must be redrafted to forbid the use of inadvertently obtained information for the purpose of initiating criminal investigations against U.S. citizens unless exigent circumstances are presented. By disallowing the use of such information for these purposes, the government would be ensuring that the NSA stays focused on its primary mission—protecting the United States from terrorism and foreign intelligence operations—and not engaging in general criminal investigations domestically. Under the current directive, the NSA has an incentive to collect as much "inadvertently acquired" information as possible. If the possibility of using such information to initiate unrelated criminal investigations were removed, the agency would cease to have an incentive to collect information unrelated to its national security mission. This would provide the agency with an incentive to maintain its focus on foreign terrorism and counterintelligence, and it would curb the temptation to stray into unrelated matters more appropriately left to those charged with domestic law enforcement.

This solution would allow the NSA to protect U.S. national security, while also enabling American citizens to communicate with foreign acquaintances without fear. It would also have the benefit of restoring public confidence in the NSA, effectively combating the perception that the agency engages in frequent violations of the very rights it was created to defend.