ELECTRONIC SURVEILLANCE IN AN ERA OF MODERN TECHNOLOGY AND EVOLVING THREATS TO NATIONAL SECURITY

Mark D. Young*

The world isn't run by weapons anymore, or energy, or money. It's run by little ones and zeroes, little bits of data. It's all just electrons.[1]

INTRODUCTION

Linking hundreds of individual computer networks has created a virtual space on which much of the world's commerce and communication now depends. Electronic mail, peer-to-peer data sharing, Voice-over-Internet Protocol (VoIP), and wireless networks are examples of the technology that enables almost unlimited access to information. This access comes with significant risk. Criminals, terrorists, hostile nation-states, and foreign industrial competitors share this ubiquitous access to information. In the industrial age, we protected ourselves with high walls and long-range weapons; in the digital age, the availability and rapid development of cyber weapons requires layers of defenses and improved awareness of adversarial capabilities and intentions.

Since the first Internet transmission on October 29, 1969 we have been deepening our dependence on digital communications.[2] There are almost two billion users of the Internet.[3] The United States economy depends on it; our critical infrastructure is controlled by it; and our national security is

* Special Counsel for Defense Intelligence, House Permanent Select Committee on Intelligence. The views expressed in this article are those of the author and do not reflect the official policy or position of any members or staff of the House Permanent Select Committee on Intelligence or any part of the U. S. government. This article is derived entirely from open source material and contains no classified information.

1. SNEAKERS (Universal Pictures 1992).

2. *See* Melissa Hathaway, Digital Dependence: Cybersecurity in the 21st Century, *Orkand Chair Distinguished Lecture Series*, UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE, http://www.umuc.edu/orkandlecture/pastlectures.shtml (last visited Feb. 5, 2010); *see also* Stuart H. Starr, *Toward A Preliminary Theory of Cyberpower*, CYBERPOWER AND NATIONAL SECURITY 43 (Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz eds., 2009).

3. INTERNET WORLD STATS (June 30, 2010), http://www.internetworldstats.com/stats.htm.

empowered by it, yet vulnerable because of it. Despite our digital dependence, our policy framework, our legal authorities, and our judicial precedent remain underdeveloped.

The cyber security legal landscape is a patchwork of federal and state statutes, federal regulation, and executive branch policy that evolved to address technologies that may no longer exist. Federal government "capabilities and responsibilities are misaligned within the U.S. government."[4] There is no shortage of threats to our information infrastructure. The media has reported that computer-controlled electric power grids are "plagued with security holes that could allow intruders to redirect power delivery and steal data . . . ."[5] Other reports claim that the Chinese military is responsible for the highly sophisticated January 2010 attack against Google's corporate network that sought to access the company's source code.[6] According to the Congressional Research Service, "[t]hreats to the U.S. cyber and telecommunications infrastructure are constantly increasing and evolving as are the entities that show interest in using a cyber-based capability to harm the nation's security interests."[7]

This Article will review the history of electronic surveillance authorities, explain how these authorities are relevant to today's cyber security issues, identify the insufficiencies of the three specific laws on this topic, and recommend discrete amendments to these statutes. The text highlights the deficiencies in the authorities governing U.S. government action in cyberspace and argues that specific sections must be amended to enhance cyber security and enable information sharing between the public and private sector. This Article does not address the federal statutes that govern cybercrime. It focuses on cyber security authorities in the national security context, but the legislative changes recommended here will also benefit law enforcement operations.

I. EVOLUTION OF ELECTRONIC SURVEILLANCE AUTHORITIES

The use of computer technology to gain intelligence or as a vector to deny, degrade, or disrupt an adversary's capabilities presents new questions for the

4. QUADRENNIAL DEFENSE REVIEW INDEPENDENT PANEL, THE QDR IN PERSPECTIVE: MEETING AMERICA'S NATIONAL SECURITY NEEDS IN THE 21ST CENTURY 61 (United States Institute of Peace 2010) [hereinafter QDR Independent Panel], *available at* http://www.usip.org/files/qdr/qdrreport.pdf.

5. Siobhan Gorman, *Grid is Vulnerable to Cyber-Attacks*, WALL ST. J., Aug. 3, 2010, at A3, *available at* http://online.wsj.com/article/SB10001424052748704905004575405741051458382.html.

6. Bill Gertz, *Inside the Ring: PLA Hack on Google?*, WASH. TIMES, July 8, 2010, at A7. *See generally* Kim Zetter, *Google Hack was Ultra Sophisticated, New Details Show*, WIRED (Jan. 14, 2010), http://www.wired.com/threatlevel/2010/01/operation-aurora.

7. JOHN ROLLINS & ANNA HENNING, CONG. RESEARCH SERV., R40427, COMPREHENSIVE NATIONAL CYBERSECURITY INITIATIVE: LEGAL AUTHORITIES AND POLICY CONSIDERATIONS 2 (2009).

laws of electronic surveillance, intelligence collection, and war.[8] In the context of the Fourth Amendment, Professor Orin Kerr of George Washington University Law School notes, "Courts have only recently begun to address these questions, and the existing legal scholarship is surprisingly sparse."[9] What is true of the scholarship in the Fourth Amendment criminal context is doubly true in the national security realm. Current scholarship is either "highly abstract or else focuses only on discrete doctrinal questions."[10]

Since computers and networks are by nature electronic devices, electronic surveillance authorities play an important role in state surveillance for both law enforcement and national security investigations. The history of electronic surveillance law is relevant to understanding how specific statutes are inconsistent with privacy and state investigations. Although there are numerous statutes that regulate government electronic surveillance,[11] this analysis focuses on the Electronic Communications Privacy Act, the Stored Communications Act, and the Foreign Intelligence Surveillance Act:

> Electronic surveillance law in the United States is comprised primarily of two statutory regimes: (1) the Electronic Communications Privacy Act ("ECPA"), which is designed to regulate domestic surveillance; and (2) the Foreign Intelligence Surveillance Act of 1978 ("FISA"), which is designed to regulate foreign intelligence gathering. While other statutes provide additional protection, ECPA and FISA are the heart of electronic surveillance law.[12]

The Fourth Amendment requires a particularized description of the places to be searched and the things to be seized.[13] Reasonableness is "the ultimate touchstone of Fourth Amendment legitimacy."[14] Because electronic surveillance authority is such a comprehensive investigatory power, the

8. *See generally* K.A. Taipale, Deconstructing Information Warfare, Presentation to Committee on Policy Consequences and Legal/Ethical Implications of Offensive Information Warfare, The National Academies (Oct. 30, 2006), *available at* http://www.information-retrieval.info/PIW/deconstructing/Taipale-IW-103006.pdf.

9. Orin Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1006 (2010).

10. *Id. See generally* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 109-10 (1999) (advocating the translation of constitutional principles to the Internet); Patricia L. Bellia & Susan Freiwald, *Law in a Networked World: Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 125 (2008); Max Guirguis, *Electronic Mail Surveillance and the Reasonable Expectation Of Privacy*, 8 J. TECH. L. & POL'Y 135, 135 (2003).

11. *See* GINA MARIE STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., 98-326, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping* (2009).

12. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 73 GEO. WASH. L. REV. 1264, 1266 (2004).

13. U.S. CONST. amend. IV; *Maryland v. Garrison*, 480 U.S. 79 (1987) (describing the particularity required in a warrant for the places to be searched); *Andresen v. Maryland*, 427 U.S. 463 (1976) (describing the permissible breadth of warranted seizures).

14. BENJAMIN WITTES, LAW AND THE LONG WAR: THE FUTURE OF JUSTICE IN THE AGE OF TERROR 233 (2008).

government's surveillance authority must be tightly controlled. Electronic surveillance records on-line behavior, social contacts, interests, and other activities that may extend beyond intended investigatory matters and for longer than is necessary for the investigatory purpose. The objective of electronic surveillance law is to limit government access to the electronic lives of U.S. citizens, while providing reasonable access for proper investigations. The law seeks to provide "oversight of government surveillance, accountability for abuses and errors, and limits against generalized forms of surveillance."[15]

Eavesdropping has existed since before the founding of the United States.[16] Electronic communication resulted in the birth of a new form of eavesdropping: electronic surveillance. The U.S. Civil War saw extensive wiretapping of Union and Confederate telegraph wires.[17] On the first day of World War I, the British cable ship *Telconia* severed German transatlantic cables in the North Sea forcing Germany to communicate in ways that the United Kingdom could monitor.

Germany was now forced to communicate with the world beyond the encircling nations of the United Kingdom, France, and Russia by radio or over cables controlled by enemies. Germany thus delivered into the hands of her foes her most secret and confidential plans, provided only that they could remove the jacket of code and cipher in which Germany had encased them.[18]

It was during World War I that the U.S. Congress enacted the first temporary federal wiretap law to prohibit the tapping or disclosure of the contents of telegraph or telephone messages.[19] After the War, the Radio Act of 1927 prohibited the interception or disclosure of private radio messages.[20]

In 1928, the first electronic surveillance case reached the U.S. Supreme Court. In *Olmstead v. United States*,[21] the Court held that the tapping of telephone wires by federal agents did not violate the Fourth Amendment since there was no "entry of the houses or offices of the defendants," and the agents only obtained the content of their conversations. In other words, no place was searched and no property was seized. Justice Brandeis was prescient in his

15. Solove, *supra* note 12, at 1270.

16. 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 169 (1769) (defining eavesdropping as a common law offense).

17. For an extensive description of wiretapping and the use of ciphers to protect from wiretapping, see DAVID KAHN, THE CODE-BREAKERS: THE COMPREHENSIVE HISTORY OF SECRET COMMUNICATION FROM ANCIENT TIMES TO THE INTERNET 214-229 (Scribner 1996).

18. *Id.* at 266.

19. *See* STEVENS & DOYLE, *supra* note 11, at 2.

20. Radio Act of 1927, Pub. L. No. 632, ch. 169, 44 Stat. 1172.

21. 277 U.S. 438 (1928); *see also* WAYNE R. LAFAVE, JEROLD H. ISRAEL, & NANCY J. KING, CRIMINAL PROCEDURE 259 (3rd ed. 2000) (It made no difference that the conduct was in violation of a state law making it a misdemeanor to "intercept" telegraphic or telephonic messages, as the statute did not declare evidence so obtained was inadmissible and, in any event, a state statue "can not affect the rules of evidence applicable in courts of the United States.").

dissent in *Olmstead*, noting:

> [t]he progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[22]

In the wake of the *Olmstead* opinion, Congress expanded the protections in the Radio Act. With the Federal Communications Act of 1934, wire communications were now also protected.[23] It said nothing, however, about the use of mechanical devices to record in-person conversations. Without this prohibition, Fourth Amendment challenges to electronic surveillance greatly increased and the increasing inventory of court opinions began to erode the trespass reasoning in *Olmstead*.[24]

In 1967, the trespass doctrine in *Olmstead* was replaced by the reasonable expectation of privacy doctrine from *Katz v. United States*.[25] It was then clear that "wiretapping and electronic eavesdropping are subject to the limitations of the Fourth Amendment."[26] A consequence of this decision is the attachment of the warrant requirement in investigations involving electronic surveillance. "To avoid constitutional problems and at the same time preserve wiretapping and other forms of electronic eavesdropping as a law enforcement tool, some of the states established a statutory system under which law enforcement officials could obtain a warrant, or equivalent court order, authorizing wiretapping or electronic eavesdropping."[27]

However, in the same year, the New York Code of Criminal Procedure, which included detailed electronic surveillance warrant requirements, was struck down by the Supreme Court in *Berger v. New York*.[28] The Court found the statute unconstitutional because it failed to require a description of the place to be searched, the crime to which the search related, and a description of the

22. *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).

23. 48 Stat. 1103-1104 (1934).

24. STEVENS & DOYLE, *supra* note 11, at 3. Initially the Court applied *Olmstead*'s principles to the electronic eavesdropping cases. Thus, the use of a dictaphone to secretly overhear a private conversation in an adjacent office offended no Fourth Amendment [precepts] because no physical trespass into the office in which the conversation took place had occurred. Goldman v. United States, 316 U.S. 129 (1942). Similarly, the absence of a physical trespass precluded Fourth Amendment coverage of the situation where a federal agent secretly recorded his conversation with a defendant held in a commercial laundry in an area open to the public. On Lee v. United States, 343 U.S. 747 (1952). On the other hand, the Fourth Amendment did reach the government's physical intrusion upon private property during an investigation, as for example when they drove a "spike mike" into the common wall of a row house until it made contact with a heating duct for the home in which the conversation occurred. Silverman v. United States, 365 U.S. 505 (1961).

25. 389 U.S. 347 (1967).

26. LAFAVE, ISRAEL & KING, *supra* note 21, at 261.

27. STEVENS & DOYLE, *supra* note 11, at 4.

28. 388 U.S. 41 (1967).

conversation to be seized. Both *Katz* and *Berger* persuaded Congress to pass the Omnibus Crime Control and Safe Streets Act of 1968.[29] Title III of the Act generally prohibited wiretapping and electronic eavesdropping, but provided federal and state law enforcement authorities some authority for electronic surveillance, albeit under strict limitations.

There was a national security exception in Title III, however. Section 2511 stated that nothing in the title

> shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect the United States against the overthrow of the government by force or other unlawful means.[30]

Congress recognized that law enforcement wiretaps were not the same as the collection of foreign intelligence and that no warrant was required for national security investigations. A decade later, the Supreme Court would invite Congress to more carefully legislate the President's surveillance powers in national security cases.

In 1972, the President's authority to conduct warrantless wiretaps was the issue in *United States v. United States District Court*,[31] where the government monitored a "domestic radical group engaged in a conspiracy to destroy federal government property" without a warrant.[32] The Court acknowledged the government's strong investigative duty in national security matters, but also noted that "Fourth Amendment protections become more necessary when the targets of official surveillance may be suspected of unorthodoxy in their political beliefs."[33] The opinion stated, "Congress may wish to consider protective standards for [domestic security surveillance] which differ from those already prescribed for specified crimes in Title III."[34]

After the Court rejected the claim of inherent presidential electronic surveillance authority in domestic national security cases, Congress amended the President's authority to collect foreign intelligence with the Foreign Intelligence Security Act of 1978 (FISA).[35] "FISA provides a procedure for judicial review and authorization or denial of wiretapping and other forms of

29. Pub. L. No. 90-351, 82 Stat. 197 (1968) (then codified at 18 U.S.C. §§ 2510-2522 (2006)) [hereinafter Crime Control Act].

30. Crime Control Act, 18 U.S.C. § 2511(3) (1970).

31. 407 U.S. 297 (1972).

32. LAFAVE, ISRAEL & KING, *supra* note 21, at 276.

33. 407 U.S. at 314; *see also* LAFAVE, ISRAEL & KING, *supra* note 21, at 276. The Court also noted that Executive Officers of the government do not qualify under the Fourth Amendment as neutral magistrates, that internal security matters are not too subtle and complex for judicial evaluation and that prior judicial approval will not fracture the secrecy essential to official intelligence gathering.

34. 407 U.S. at 322.

35. 50 U.S.C. §§ 1801-1862 (2006).

electronic eavesdropping for purposes of foreign intelligence gathering."[36] It also created the Foreign Intelligence Surveillance Court as a judicial venue to adjudicate executive surveillance applications, with emergency authority provided to the Attorney General.

After the September 11, 2001 terrorist attacks, FISA was criticized for excessively limiting law enforcement personnel's access to FISA surveillance data.[37] These restrictions became known as the FISA "wall." "[This] wall addressed the concern that law enforcement and prosecutorial personnel might use the FISA instrument, or information obtained from FISA surveillance, to either negate the necessity of a Title III order or to develop the probable cause to get one."[38]

Within their response to the September 11 terrorist attacks, known as the PATRIOT Act, Congress sought to remove the wall by changing the FISA certification requirement.[39] Previous interpretation of FISA meant that the sole-purpose of the surveillance must be to obtain foreign intelligence. "As a result, guidelines since the 1980s and across administrations had limited the extent to which the [Department of Justice] criminal division could direct and receive foreign intelligence surveillance."[40] The PATRIOT Act changed the certification requirement of foreign intelligence collection from a "sole-purpose test" to a "significant-purpose test."[41] With this amendment, government officers could now use FISA for electronic surveillance that had both an intelligence and law enforcement objective.

FISA was amended twice more, once in 2007 by the Protect America Act[42] and again in 2008 with the Foreign Intelligence Surveillance Act of 1978 Amendments Act.[43] The 2008 legislation repealed the Protect America Act and remains in effect. It provides authority to collect foreign intelligence on overseas targets,[44] it reaffirms that FISA and Title III are the exclusive authorities for electronic surveillance,[45] and it protects from civil liability

36. STEVENS & DOYLE, *supra* note 11, at 5.

37. JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 84-85 (2007).

38. *Id*. at 85.

39. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 [hereinafter USA Patriot Act] (codified in scattered titles of the U.S. Code).

40. *Id.*; *see also In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

41. USA Patriot Act, 50 U.S.C. § 1804(a)(7)(b) (2002).

42. Pub. L. No. 110-55, 121 Stat. 552.

43. Pub. L. No. 110-261, 122 Stat. 2436 (2008).

44. 50 U.S.C. §§ 1881-1881g (2006).

45. *See* STEVENS & DOYLE, *supra* note 11, at 49, n.241 (quoting 50 U.S.C. § 1812: "(a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of title 18, United States Code, and this Act shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted. (b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an

commercial entities that assist with government surveillance.[46]

For law enforcement electronic surveillance, Congress amended Title III with the Electronic Communications Privacy Act (ECPA) in 1986.[47] The amended law attempted to balance privacy interests and law enforcement needs, but it also showed Congress's support of the expanding communications technology industry.[48] The statute included "new protection and law enforcement access provisions for stored wire and electronic communications and transactional records access (e-mail and phone records), and for pen registers as well as trap and trace devices (devices for recording the calls placed to or from a particular telephone)."[49] The ECPA enhanced Title III to incorporate new forms of electronic communication, such as e-mail. It also provided protection beyond message transmission to those communications stored in computer systems.[50]

Title II of the ECPA is known as the Stored Communications Act.[51] This section regulates law enforcement access to electronically stored communications[52] and to "subscriber records of various communications service providers, such as [Internet Service Providers (ISPs)]."[53] The law defines electronic storage as "any temporary, intermediate storage" that is "incidental" to the communication and "any storage of such communication by an electronic communications service for purpose of backup protection of such communication."[54] This definition means that e-mail that is on the ISP's computers but has yet to be accessed by the recipient is considered to be in "electronic storage." Once accessed, the recipient may still maintain copies of the e-mail on the ISP's server.

The Stored Communications Act distinguishes communications that have been stored for more than six months. "Government officials may gain access to wire or electronic communications in electronic storage for less than six months under a search warrant issued upon probable cause to believe a crime has been committed and the search will produce evidence of the offense."[55] A warrant is required if the ISP customer or subscriber is not to be notified of the

amendment to this Act or chapters 119, 121, or 206 of title 18, United States Code, shall constitute an additional exclusive means for the purpose of subsection (a)").

46. 50 U.S.C. § 1885-1885c (2006).

47. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified at 50 U.S.C. §§ 1801-1862 (2006)) [hereinafter ECPA].

48. STEVENS & DOYLE, *supra* note 11, at 5 (Senate Report 541 mentioned that threats to privacy in these new communications media "may unnecessarily discourage potential customers from using innovative communications systems") (internal citation omitted).

49. *Id.* at 5-6.

50. Solove, *supra* note 12, at 1716.

51. 18 U.S.C. §§ 2701-2712 (2006).

52. 18 U.S.C. § 2510(17) (2006).

53. Solove, *supra* note 12, at 1722 (citing 18 U.S.C. § 2510(17)(B) (2006)).

54. *Id.* (citing 18 U.S.C. § 2510(17) (2006)).

55. STEVENS & DOYLE, *supra* note 11, at 39.

government access to the communications, or government accesses communications older than six months, or communications stored on remote computers.[56]

II. ELECTRONIC SURVEILLANCE AND CYBERSPACE

The electronic surveillance authorities discussed above are relevant to national security investigations because computer servers and ISPs are provided privacy protections under U.S. law and there is an expanding possibility that terrorists will hold dual citizenship. An example of the unique circumstances under which federal law enforcement and the American intelligence community must now operate is the status of Anwar al-Awlaki. This radical Muslim cleric was born in New Mexico in 1971. As an illustration of the significance of the dual citizenship issue, there has been recent debate about the Obama administration's authorization for the targeting and killing of al-Awlaki.[57]

These statutes are also relevant to U.S. cyber activities because of the definition of electronic surveillance:

> The acquisition by an *electronic, mechanical, or other surveillance device of the contents of any wire or radio communication* sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[58]

The definition also includes the collection of communications content if it occurs *within* the United States.[59] Thus, if the government wanted to see the content of an e-mail sent from al-Awlaki to a recipient in Saudi Arabia, but collected the e-mail from somewhere within the United States, the collection is electronic surveillance and subject to the limitations of electronic surveillance law. The definition means that national security and law enforcement investigations, which include online monitoring, are subject to the Fourth Amendment and the regulations that have evolved with electronic surveillance

56. 18 U.S.C. § 2703(a), (b)(1)(A), (b)(2) (2006).

57. Scott Shane, *U.S. Approves Targeted Killing of American Cleric*, N.Y. TIMES, Apr. 6, 2010, at A12, *available at* http://www.nytimes.com/2010/04/07/world/middleeast/07yemen.html?_r=1.

58. ECPA, 50 U.S.C. § 1801(f)(1) (2006) (emphasis added).

59. *Id.*; 18 § U.S.C. 2511(2)(i) (2006) ("It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if - (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer; (II) the person acting under color of law is lawfully engaged in an investigation; (III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and (IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.").

authorities.

The final parts of the electronic surveillance definition accommodate the decision in *Katz* incorporating the acquisition of the contents of any communication "*in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes*, and if both the sender and all intended recipients are located within the United States."[60]

According to a National Defense University International Cyber Security Conference:

> The first requirement when seeking to coalesce cyberspace governance is the recognition that spoken and written words form the foundation of our understanding of cyberspace and its governance. As such we need to come up with clear definitions if effective governance is to exist. We also need a common lexicon and broader understanding of criminal threats, governance tools and what constitutes cyber security.[61]

The cyber lexicon remains confusing. The Department of Defense's *Dictionary of Military and Associated Terms* originally defined cyberspace as "the notional environment in which digitized information is communicated over computer networks."[62] The definition was amended in 2008 to a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[63]

A new definition of cyber space has been published by the Vice Chairman of the Joint Chiefs of Staff: "[A] [d]omain characterized by the use of electrons and the electromagnetic spectrum to store, modify, and exchange data via network[ed] systems and associated physical infrastructures."[64] There are myriad definitions of cyberspace—and associated terms—that confuse the issues within the federal government.[65]

According to a cyber security workshop hosted by the American Bar

60. ECPA, 50 U.S.C. § 1801(f)(1) (2006) (emphasis added).

61. Chuck Barry, Lauren Lee & Marek Rewers, INTERNATIONAL CYBER SECURITY CONFERENCE FINAL REPORT 4 (2009), *available at* http://www.ndu.edu/CTNSP/docUploaded/Cyber%20International%20Cyber%20Security%20Conf%20Final%20Report.pdf.

62. JOINT CHIEFS OF STAFF, JOINT PUB. 1-02: DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 110 (2001), *available at* http://www.bits.de/NRANEU/others/jp-doctrine/ jp1_02(01).pdf.

63. JOINT CHIEFS OF STAFF, JOINT PUB. 1-02: DEPARTMENT OF DEFENSE DICTIONARY OF MILITARY AND ASSOCIATED TERMS 140 (2008), *available at* http://www.militarynewsnetwork.com/publications/militaryterms.pdf.

64. Memorandum from the Vice Chairman of the Joint Chiefs of Staff to the Chiefs of the Military Services, Commanders of the Combatant Commands, and Directors of the Joint Staff Directors, Joint Terminology for Cyberspace Operations 7 (undated).

65. *See* DANIEL T. KEUHL, *From Cyberspace to Cyberpower: Defining the Problem*, *in* CYBERPOWER AND NATIONAL SECURITY 24-31 (Franklin D. Kramer, Stuart H. Starr & Larry K. Wentz eds., 2009).

Association's Standing Committee on National Security, the National Strategy Forum, and the McCormick Foundation, "the laws of intelligence collection have applicability to our cyber activities in two contexts: as rules of authorization and limitation within the domestic sphere and as rules of public disclosure."[66] The workshop report acknowledges the intelligence community's concerns about cyber vulnerabilities that may enable adversarial cyber intrusions. The intelligence community may share cyber vulnerability information within the U.S. government, but current law prohibits the government from disclosing the same information to the private sector. In the cyber domain—most of which is owned by the private sector—information sharing between the government and private sector is largely prohibited. "This is one legal area that clearly requires work."[67]

The definitions of cyber space are illustrative of the different understandings held by different parts of the government. It is difficult to discuss the privacy, policy, and legal issues surrounding the national security sector's cyber activities if no one agrees on what cyber space is. The inconsistent understanding compounds the challenge of discussing how electronic surveillance should be regulated. Cyber investigations are a significant instrument for monitoring terrorist and adversarial state activity, but without at least a general understanding of cyber space and how much government activity is appropriate in cyber space, we are less secure and may be providing criminals and terrorist an online sanctuary.

A. Legal Insufficiencies

The government is attempting to protect national interests from myriad cyberspace threats and shift its organizational structures to better manage its limited cyberspace resources. It is doing this, however, without adjusting one of the biggest cyber vulnerabilities facing the country: insufficient legal authorities to allow federal action in the cyber domain. According to the Quadrennial Defense Review (QDR) Independent Panel, established by Congress "to review the QDR, assess the long term threats facing America, and produce recommendations regarding the capabilities which will be necessary to meet those threats,"[68] national security planners must use a comprehensive approach to address current threats. The panel recommended a review and

66. ABA STANDING COMM. ON LAW AND NAT'L SEC. AND NAT'L STRATEGY FORUM, NATIONAL SECURITY THREATS IN CYBERSPACE 16 (SEPT. 2009), *available at* http://nationalstrategy.com/Portals/0/National%20Security%20Threats%20in%20Cyberspace%20%20FINAL%2009-15-09.pdf.

67. *Id.* at 17. The Economic Espionage Act of 1996 is available for domestic purposes, but it has been an underutilized tool of law enforcement. *See* Harvey Rishikof, *Economic and Industrial Espionage*, *in* VAULTS, MIRRORS & MASKS (Jennifer E. Simms & Burton Gerber eds., 2009).

68. QDR Independent Panel, *supra* note 4, at iv.

restructure of the laws governing the armed forces and national defense. To better address cyber threats aligning against U.S. interests, criminal statutes must be included in any analysis that seeks to improve interagency coordination and clarification of departmental and agency authorities and responsibilities.

The first and most significant cyber policy issue in the national security arena concerns covert action. There is ongoing debate among government lawyers about the Pentagon's legal authority to disrupt a foreign network during peacetime operations. "The CIA has argued that doing so constitutes a 'covert' action that only it has the authority to carry out, and only with a presidential order."[69] Others argue that the Defense Department can conduct traditional military activities online.[70]

The extant legal authorities governing cyber activities within the Department of Defense provide insufficient statutory authority for military cyber operations. According to General Keith Alexander, the Commander of U.S. Cyber Command and the Director of the National Security Agency, "offensive [cyber] capabilities must be based on 'the rule of law.'"[71]

The Department of Defense believes its current authority provides significant intelligence authority to the Secretary of Defense. Title 10 is vague about the intelligence responsibilities of the Secretary of Defense.[72] Title 50 acknowledges that the Defense Department conducts intelligence operations in support of military operations. It also mandates that the Secretary of Defense ensure that "the tactical intelligence activities of the Department of Defense complement and are compatible with the intelligence activities under the National Intelligence Program."[73] The lack of clarity in the authorities of the Department of Defense exacerbates the challenges of cyber operations. If it is unclear whether the clandestine collection of information from a foreign

69. Ellen Nakashima, *Pentagon Considers Preemptive Strikes as Part of Cyber-Defense Strategy*, WASH. POST, Aug. 28, 2010, at A1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/08/28/AR2010082803849.html.

70. *See generally* Chairman of the Joint Chiefs of Staff, NATIONAL MILITARY STRATEGY FOR CYBERSPACE OPERATIONS 1, 2 (December 2006), *available at* http://www.dod.mil/pubs/foi/ojcs/07-F-2105doc1.pdf (stating the Department of Defense will "execute the full range of military operations (ROMO) in and through cyberspace to defeat, dissuade, and deter threats against US interests.").

71. Nakashima, *supra* note 69.

72. *See* Exec. Order No. 13,470, 3 C.F.R. 218, 232-33 (2008) (§ 1.10(a)-(k)). Exec. Order 12333 (now Exec. Order 13,470) does specify some intelligence responsibilities of the Secretary of Defense, such as "[c]ollect (including through clandestine means), analyze, produce, and disseminate information and intelligence and be responsive to collection tasking and advisory tasking by the Director," *id.* at 232 (§ 1.10(a)); and "[c]ollect (including through clandestine means), analyze, produce, and disseminate defense and defense-related intelligence and counterintelligence, as required for execution of the Secretary's responsibilities. *Id.* (§ 1.10(b)).

73. 50 U.S.C. § 403-5(3) (2006).

computer network is "defense-related intelligence," then it will be unclear whether it is within the Defense Department's authority to collect that information. It also remains to be decided if computer network operations should be classified as covert action.

Covert action is "an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly."[74] It does not include "activities the primary purpose of which is to acquire intelligence" or "traditional diplomatic or military activities or routine support to such activities."[75] The term *traditional military activity* is not defined by statute or military doctrine. The inherent anonymity of actions in cyberspace does not mean the operation is a covert action, merely because the Defense Department fails to acknowledge its involvement publicly. As a policy matter, we must decide into which category the online activities of our military and intelligence agencies belong. Without this policy decision, our ability to use cyberspace to protect American interests is significantly burdened. We must decide if everything each of the elements of our national security community does on computer networks is subject to electronic surveillance law.

Second, we must reconsider our concept of online privacy. Within a relatively short period of time, there have been significant shifts in what different age groups consider private.

Younger "Digital Natives" have a culture of sharing built though forwarded e-mails and social-networking site posts. Their idea of privacy is different from older "digital immigrants." Digital natives have:

> [O]ver 10,000 hours playing videogames, over 200,000 emails and instant messages sent and received; over 10,000 hours talking on digital cell phones; over 20,000 hours watching TV (a high percentage fast speed MTV), over 500,000 commercials seen—all before the kids leave college. And, maybe, *at the very most*, 5,000 hours of book reading.[76]

Cyber security presents novel issues that cut across areas of law that have successfully represented our national values, but now may not be appropriate for current technology. We may have to review how much Fourth Amendment protection we provide to online activity. The legal regimes governing electronic surveillance have unsuccessfully tried to remain current with modern technology. The Supreme Court's opinion in *Katz v. United States* notwithstanding, some argue that the Fourth Amendment should not protect some forms of online communications. Professor Orin Kerr argues that the "contents of online communications ordinarily should receive Fourth

74. *Id.*

75. 50 U.S.C. § 413b(e) (2006).

76. Marc Prensky, *Digital Natives, Digital Immigrants, Part II: Do They Really* Think *Differently?*, ON THE HORIZON, Oct. 2001, at 1.

Amendment protection but that non-content communications should not be protected."[77] "Online, non-content surveillance is usually surveillance related to identity, location, and time; content surveillance is surveillance of private thoughts and speech."[78]

The distinction between government surveillance of activities within enclosed spaces and government surveillance in public space is applicable to government surveillance online. "So long as conduct is out in the open, it is not protected by the Fourth Amendment."[79] In contrast, "entering enclosed spaces ordinarily constitutes a search that triggers the Fourth Amendment."[80] The inside/outside distinction in the physical domain should be applied as a content/non-content distinction in the cyber domain.

Internet surveillance of non-content information should not trigger the Fourth Amendment just like surveillance of public spaces does not trigger the Fourth Amendment. Surveillance of content should presumptively trigger the Fourth Amendment in the Internet setting just like surveillance of inside spaces presumptively triggers the Fourth Amendment in the physical world.[81]

Kerr does acknowledge that the difference between content and non-content information can be difficult to determine.[82] Adopting the content/non-content distinction, however, would be useful in evolving electronic surveillance laws that are critical to ensure the national security community has both adequate legal authorities with which to apply its evolving cyber capabilities. It would put the military and intelligence agencies on firmer foundations to conduct cyberspace activities.

Some critics of the content/non-content paradigm argue that Internet surveillance is less-expensive, easier to conduct, and much more invasive than conventional surveillance. While this may be true in some circumstances, "online surveillance varies greatly in its ease, cost, and invasiveness: it can be cheap, easy and highly invasive, or it can be expensive, difficult, and much less invasive than physical surveillance."[83] The expanding use of commercially available encryption, anonymizers, and proxy servers makes Internet surveillance much more difficult, expensive, and time consuming.

77. Kerr, *supra* note 9, at 1007-08.

78. *Id.* at 1018.

79. *Id.* at 1010.

80. *Id.*

81. *Id.* at 1018.

82. Kerr notes that the subject line, the body of the message, and any attachments of an electronic mail are contents of the communication, while the "to/from" address and the size of the e-mail are non-content information. *Id.* at 1023.

83. *Id.* at 1032.

B. Electronic Surveillance Insufficiencies Hinder U.S. Cyber Security Efforts

Laws that set the boundaries of government cyber activity include the Electronic Communications Privacy Act, the Stored Communications Act, the Foreign Intelligence Surveillance Act, the Computer Fraud and Abuse Act, the Federal Information Security Management Act, the Communications Assistance for Law Enforcement Act, and the laws governing intelligence collection. None of these laws provide adequate guidance, flexibility, or privacy protections for the national security community charged with protecting the nation and its critical infrastructure from cyber exploitation or attack. The President's National Security Telecommunications Advisory Committee recognizes the significant legal impediments that may exist to appropriate cyber security information sharing.[84]

Although each of these statutes should be amended to enhance U.S. cyber security, the priority should be amendments to the Electronic Communications Privacy Act (ECPA), the Stored Communications Act (SCA), and the Foreign Intelligence Surveillance Act (FISA). Elements of the ECPA encumber information sharing between the government and the private sector. The SCA restricts the disclosure of data before it is accessed by the recipient or if it is left in storage by the recipient.[85] Like the ECPA, the SCA may prevent ISPs from sharing metadata or content from the draft folder of a terrorist's e-mail account with the national security community for fear of criminal or civil liability.[86] Amended in 2008, FISA's provisions created an unintentional gap in the government's cyber capabilities. Congress amended FISA in a way that may require the loss of collection by intelligence agencies at the exact instant when the need for intelligence on the intentions of a target is highest.

84. *See* THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE, CYBERSECURITY COLLABORATION REPORT: STRENGTHENING GOVERNMENT AND PRIVATE SECTOR COLLABORATION THROUGH A CYBER INCIDENT DETECTION, PREVENTION, MITIGATION, AND RESPONSE CAPABILITY I, 15 (2009), http://www.ncs.gov/nstac/reports/2009/NSTAC CCTF Report.pdf.

85. Electronic storage is "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(a)-(b).

86. Nicholas Matlach, *Who Let the Katz Out? How the ECPA and the SCA Fail to Apply to Modern Digital Communications and How Returning to the Principles in* Katz v. United States *Will Fix It*, 18 COMMLAW CONSPECTUS 421, 449 (2010).

1. Electronic Communications Privacy Act

The National Security Strategy prioritizes the prevention of nuclear weapons proliferation to violent extremists.[87] Counterterrorism operations have been an obvious priority since September 11, 2001. The United States has a clear interest in deterring terrorism; in order to do that, the national security elements of the federal government must have adequate authority to investigate terrorists and act once they are discovered.

Modern technologies provide a means of coordination for terrorists, just as they make communication and commerce more convenient. The technology provides anonymity, convenience, and rapid communication. E-mail, peer-to-peer connections, voice over internet protocol (VoIP), and social networks such as Facebook and MySpace provide forums for extremists to share their ideologies and their techniques and procedures for conducting illicit activities.

With the enactment of the ECPA,[88] Congress sought to adapt privacy protections to technologies that were new in 1986.[89] The statute was effective in protecting communications privacy until technology and network structures developed in such a way as to hinder reasonable law enforcement and national security investigations. Modern technology has made ECPA "unwieldy and unreliable . . . immensely difficult for judges and investigators to apply, confusing, costly, and full of legal uncertainty for communications and other technology tools and service providers, and an unpredictable guardian of our country's long cherished privacy values."[90] The confusion with ECPA also has an impact on national security investigations. Under ECPA, government access to an e-mail from a potential terrorist is subject to different legal standards depending on when the recipient accessed the e-mail. [91] If the e-mail is stored and has not yet been accessed by its recipient, ECPA requires a warrant for the government to see its contents.[92] Once the same e-mail is opened, the government may access the content with a subpoena.[93] Although there is disagreement among circuit courts on this "open and unopened" communications distinction, according to the Department of Justice, the

87. EXECUTIVE OFFICE OF THE PRESIDENT, NATIONAL SECURITY STRATEGY 4 (2010), http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

88. ECPA, 50 U.S.C. §§ 1801-1862 (2006); *see also* S. REP. NO. 99-541, at 1 (1986).

89. Matlach, *supra* note 86, at 442; *see also* S. REP. NO. 99-541, at 1.

90. J. Beckwith Burr, The Electronic Communications Privacy Act of 1986: Principles of Reform 3 (WilmerHale, Memorandum), http://digitaldueprocess.org/files/DDP_Burr_Memo.pdf.

91. *See* Robert Gellman, Privacy in the Clouds: Risks to Privacy and Confidentiality from the Cloud Computing 12-13 (2009), *available at* http://www.scribd.com/doc/12805751/Privacy-in-Cloud-Computing-World-Privacy-Council-Feb-2009 (describing the struggle courts have had applying ECPA to situations not contemplated by the law's drafters).

92. 18 U.S.C. § 2703(a) (2006).

93. 18 U.S.C. § 2703(b)(1)(B) (2006).

government may subpoena the e-mail contents if they are more than 180 days old.[94] "The different standards are the unanticipated byproduct of technology changes, and not a careful balancing of the needs of law enforcement and the privacy rights of individuals."[95] Issuance of a wiretap warrant requires probable cause, but ECPA requirements "prohibit[] law enforcement from using wiretaps in the early stages of an investigation and make it one of the hardest warrants to obtain."[96] The needs of the national security community are similarly impacted by these ambiguous standards.

The ECPA applies to all online communications. It includes VoIP communications.[97] The "by the aid of wire, cable, or other like connection" requirement includes wireless connections such as mobile phones, satellites, and fiber-optic cables.[98] The law also protects communications that are "furnished or operated by any person engaged in providing or operating such facilities" for communications.[99] In the computer context, "software installed on two computers may be the 'facility' for communication."[100]

Any federal law enforcement or intelligence activity online will implicate ECPA. However, sections of ECPA are clearly inconsistent with U.S. national security. Most agree that federal cyber security efforts must include better partnering between the federal and private sectors.[101] According to Melissa Hathaway, former Acting Senior Director for Cyberspace at the National Security Council, "the ISPs want to provide threat data, but the government either can't take it or won't."[102] Lawyers for the major data providers interpret the ECPA to prohibit the voluntary provision of customer data. In some cases, "the government won't take the [threat] information because they have no technical way to receive it."[103] Hathaway explained that various providers format their information differently and that the national security sector cannot receive, store, or analyze the large volumes of information even if the ISPs did make it available to the government.

It is understandable why the private sector is concerned about breaking this law. Criminal violations of ECPA may make an offender liable for fines or up

94. Burr, *supra* note 90 at 8.

95. *Id.*

96. Matlach, *supra* note 86 at 443.

97. 18 U.S.C. § 2510(18) (2006); *see also* S. REP. NO. 99-541, at 16 (1986).

98. S. REP. NO. 99-541 at 12.

99. 18 U.S.C. § 2510(1) (2006).

100. Matlach, *supra* note 86, at 445.

101. *See, e.g.*, NATIONAL SECURITY THREATS IN CYBERSPACE, *supra* note 66, at 23; INTELLIGENCE AND NATIONAL SECURITY ALLIANCE, ADDRESSING CYBER SECURITY THROUGH PUBLIC-PRIVATE PARTNERSHIP: AN ANALYSIS OF EXISTING MODELS (2009), http://insaonline.org/assets/files/CyberPaperNov09R3.pdf.

102. Interview with Melissa Hathaway, Former Acting Senior Dir. for Cyberspace, Nat'l Sec. Council, in D.C. (Sept. 8, 2010).

103. *Id.*

to five years in prison, or both.[104] Civil liability includes injunctive or declaratory relief, and damages of at least $10,000.[105]

Under § 2702 of ECPA, civil liability attaches for the unlawful disclosure of communications data by service providers.[106] Notwithstanding the extensive list of exceptions and defenses to this liability,[107] service providers are less willing to provide data to the government after the controversy and legal suits that followed the December 2005 disclosure of the Terrorist Surveillance Program at the National Security Agency.[108] Litigation against the service providers for allegedly unlawfully providing customer data to the government continues today.[109] The legal issue with the TSP arose "because the data NSA tapped reportedly came in by fiber-optic cable, so FISA applied unless the physical tap took place outside the sovereign territory of the United States – a few miles offshore for example."[110]

The statute prohibits wiretapping and electronic surveillance in certain circumstances. "An interception can only be a violation of ECPA if the conversation or other form of communication intercepted is among those kinds which the statute protects, in oversimplified terms – telephone (wire), face-to-

104. 18 U.S.C. § 2511(4)(a) (2006).

105. 18 U.S.C. § 2520(b)-(c) (2006).

106. Stevens & Doyle, *supra* note 11, at 29; *see also* 18 U.S.C. § 2702(a) (2006).

107. Section § 2702(b) requires that

> [a] provider described in subsection (a) may divulge the contents of a communication – (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient; (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title; (3) with the lawful consent of the originator or an addressee or intended recipient of such communication, *or the subscriber in the case of remote computing service*; (4) to a person employed or authorized or whose facilities are used to forward such communication to its destination; (5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; (6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990; (7) to a law enforcement agency – (A) if the contents – (I) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime; (8) to a Federal, State, or local government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

18 U.S.C. § 2702(b) (2006). The Ninth Circuit recently explained that while a remote computer service provider may disclose to a subscriber (as noted in italics above), an electronic service provider, such as one who provides text messaging services, may not, even when the material disclosed resides in storage. Quon v. Arch Wireless Operating Co. Inc., 529 F.3d 892, 900-01 (9th Cir. 2008).

108. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at*, http://www.nytimes.com/2005/12/16/politics/16program.html.

109. *See generally* Charlie Savage & James Risen, *Federal Judge Finds N.S.A. Wiretaps Were Illegal*, N.Y. TIMES, Mar. 10, 2010, at A1, *available at*, http://www.nytimes.com/2010/04/01/us/01nsa.html.

110. WITTES, *supra* note 14, at 235.

face (oral), and computer (electronic)."[111] "Surreptitious 'access' is at least as great a threat as surreptitious 'interception' to the patrons of electronic mail (e-mail), electronic bulletin boards, voice mail, pagers, and remote computer storage."[112]

These sections that limit the interception of, access to, and disclosure of data in transmission require amendments in order to better protect the privacy of American citizens while allowing the national security community to remain current with the online activities of adversaries. Amendments to § 2702 allowing more flexibility for the ISPs would reduce their reluctance to share threat data with the government. As previously noted, "while a failure to follow the ECPA in obtaining e-mail information may not result in suppression of the evidence, it may result in civil liability for ECPA violators."[113]

The Department of Justice's Office of Legal Counsel has opined that an ISP may not even disclose its relationship with a customer without a national security letter.[114] According to this opinion, "when the FBI identifies a subscriber by name, section 2702(a)(3) [of the ECPA] forbids a provider from divulging the existence of that person's or entity's subscription with the provider."[115] ECPA also prohibits ISPs from identifying a customer if the FBI provides a phone number instead of a name. Without consent from a customer, ECPA prohibits the voluntary provision of information by the ISPs. In some cases, it even limits what can be provided by the ISPs with a national security letter.

Section 2709(b)(1) limits what the FBI can request and what an ISP may provide under a national security letter to the name, address, length of service, and local and long distance toll billing records of a person or entity.[116] The structure of the statute also supports these limitations on the sharing of subscriber information: "Section 2709 is an exception to the background rule of privacy established by 18 U.S.C. § 2702(a), which bars a provider from giving the Government a record or other information pertaining to a subscriber or customer."[117] Private defendant suits are still being litigated against telecommunications companies after the disclosure of the TSP.[118] Despite the

111. STEVENS & DOYLE, *supra* note 11, at 11.

112. *Id.* at 28. *See also* 18 U.S.C. §§ 2701-2711 (2006).

113. Am. Prosecutors Research Inst., The ECPA, ISPs, and Obtaining Email: A Primer for Local Prosecutors, (July 2005), http://www.ndaa.org/pdf/ecpa_isps_obtaining_email_05.pdf.

114. *See* Office of Legal Counsel, Requests for Information Under the Electronic Communications Privacy Act Memorandum Opinion for the General Counsel Federal Bureau of Investigation (Nov. 5, 2008), *available* http://www.justice.gov/olc/2008/fbi-ecpa-opinion.pdf.

115. *Id.* at 11.

116. 18 U.S.C. § 2709(b)(1) (2006).

117. Office of Legal Counsel, *supra* note 114, at 3.

118. Robert M. Chesney, Nat'l Security Admin., *Litigation, and the State Secrets Privilege*, *in* LEGAL ISSUES IN THE STRUGGLE AGAINST TERROR 123 (John Norton Moore &

outcome of past and pending TSP litigation, private sector companies are less likely to assist the government in law enforcement or national security investigations if their cooperation risks a civil suit.

Any amendments permitting a less burdensome regime for government access to information, for which the public believes it has an expectation of privacy, may cause civil liberties concerns, but these may be mitigated through a statutory definition of the types of data the ISPs could share and the setting of guidelines under which the data could be shared. For example, the Communications Assistance for Law Enforcement Act (CALEA) was created to ensure that telecommunications companies had the capabilities "to assist law enforcement in conducting digital electronic surveillance regardless of the specific telecommunications systems or services deployed."[119]

A similar approach should be used to allow the ISPs to share either metadata or content data with the government. An amended ECPA could include a provision that allows the disclosure of customer information, describing imminent acts dangerous to human life that are violations of the criminal laws of the United States, and not protected by the First Amendment to the U.S. Constitution. If the information describes imminent activity to "intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; [or] to affect the conduct of a government by mass destruction, assassination or kidnapping" ISPs should not be held liable for disclosing this information without a court order.[120] Such an amendment could outline the process by which the government should work with the ISPs to enhance their ability to detect threats to national security.

2. Stored Communications Privacy Act

Title II of the ECPA regulates access to stored communications and records.[121] It distinguishes between data in transit and data at rest. These distinctions are artificial, however, in light of the development of technology such as cloud computing[122] and remote computing services. "Today, the distinctions between and among data in transit, data in electronic storage, data stored by a remote computing service, and data more [than] 180 days old no

Robert Turner eds., 2010).

119. PATRICIA MOLONEY FIGLIOLA, CONG. RESEARCH SERV., RL 30677, DIGITAL SURVEILLANCE: THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT 2 (2007), *available at* http://www.law.umaryland.edu/marshall/crsreports/crsdocuments/RL30677_06082007.pdf.

120. USA Patriot Act § 802 (codified at 18 U.S.C. 2331 (2006)).

121. 18 U.S.C. §§ 2701–2711 (2006).

122. PATRICIA MALONEY FIGLIOLA, ANGELE A. GILROY & LENNARD G. KRUGER, CONG. RESEARCH SERV., RL 40230, THE EVOLVING BROADBAND INFRASTRUCTURE: EXPANSION, APPLICATIONS, AND REGULATION 9 (2009), *available at* http://assets.opencrs.com/rpts/R40230_20090219.pdf.

longer conform to the reasonable expectations of Americans, nor do these distinctions serve the public interest."[123] These distinctions are irrelevant in the context of national security operations. "The SCA prohibits the unauthorized access to an electronic communication service or facility 'and thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communications while it is in electronic storage.'"[124] Thus, "when a communication is in transmission between the source and the destination, the ECPA governs."[125] However, when a communication reaches its destination, the SCA governs.[126]

Arguing against an "automobile-exception"[127] to the Fourth Amendment warrant requirement for computer information, Orin Kerr argues that "computer data moves in a very different sense than automobiles or ships move."[128] In contrast to what occurs when law enforcement officers lose track of a vehicle in the process of getting a warrant, computer data is copied, rather than being physically moved. "When a file is transferred from one place to another, a new copy is generated and that new copy is sent to the new place. The old copy is ordinarily left behind. Further, when a copy is made, that copy can be controlled and protected from interference." Kerr concludes that, since the data remains on a computer, the government "can copy the data—or order a copy to be made by the server that hosts the data—and then access the copy at a later time."[129] Because the data is not destroyed and is still accessible, "there is no general exigency that justifies a rule that the government can access

123. Burr, *supra* note 90, at 9.

124. Matlach, *supra* note 86, at 448.

125. *See* United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) (noting "when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time").

126. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1072-73 (9th Cir. 2004) (noting that the SCA "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a (continued) communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents . . . the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility").

127. States may allow the warrantless search of an automobile, except for the trunk, if the police officer reasonably believes that the vehicle holds evidence of a crime. The U.S. Supreme Court has determined that this exception is not a violation of the Fourth Amendment because drivers have a "reduced expectation of privacy" and because a vehicle is inherently mobile. This reduced expectation of privacy also allows police officers with probable cause to search a car to inspect drivers' and passengers' belongings that are capable of concealing the object of the search, even if there is no proof that the driver and passenger were engaged in a common enterprise. Wyoming v. Houghton, 526 U.S. 295 (1999).

128. Kerr, *supra* note 9, at 1041.

129. *Id.* at 153. This occurred in United States v. Gorshkov, No. CR00-550C, 2001 WL 1024026 (W.D. Wash. May 23, 2001), where the target had left his hacker tools on a server in Russia. FBI agents in the United States remotely accessed the account, copied the folder containing the tools, and downloaded it to a file in the United States. However, the agents did not actually open the file until they had obtained a warrant.

Internet communications without a warrant."[130]

However, Professor Kerr underestimates the operational security practices of terrorists and criminals. Commercially available encryption, proxy-servers, unknown e-mail accounts, and small, highly concealable storage media negate Kerr's argument. Data can disappear, or be made inaccessible in seconds. Computer hard drives can be destroyed in five seconds,[131] and small storage media can hold eight gigabits of data on a device no larger than a quarter.[132] Because data can quickly be made inaccessible, there should be an exigency exception for the warrant requirement for computer data. In the national security context, warrants are inappropriate in cases where a U.S. citizen is not the target of the investigation. If the investigation does involve an entity protected by the Fourth Amendment, then there should be a legal accommodation to access fleeting data without an *a priori* warrant application.

The distinction between stored and transit data may not be as relevant today as it was when the SCA was passed, but the statute also distinguished between electronic communications service providers and remote computing service providers.[133] Each is subject to distinct exceptions for consent disclosures. Communications content may be disclosed with consent from only one party to the communication. In contrast, remote computing service providers . . . may also disclose with the consent of a subscriber to the service.[134] In 2008, the Ninth Circuit held that the provider of a text messaging service was an electronic communications service provider rather than a remote computing service provider, and consequently, it was in violation of the Section 2702 when it disclosed to the city-subscriber the content of messages sent to and from a city employee's pager.[135]

There is little judicial consensus concerning how SCA should be applied to contemporary communications. The difficulty flows from the fact that the definitions used for terms in section 2703 were crafted for the technology of an earlier day. Application becomes an issue because under one construction the content of electronic communications can only be secured under a warrant; under another, a subpoena will suffice; and under a third, the required disclosure provisions of section 2703 do not apply at all.

130. Kerr, *supra* note 9, at 1041.

131. *See* Ryan DeBeasi, *How to Destroy a Hard Drive in Five Seconds*, NETWORKWORLD.COM, June 27, 2006, *available at* http://www.networkworld.com/news/2006/062706-guard-dog.html.

132. *See generally* DT's Flash Drive Blog (Apr. 24, 2009), http://www.usbmemorystick s.net/smallest-nano-flash-drives.

133. *See* 18 U.S.C. § 2702(a)(1)-(2) (2006).

134. 18 U.S.C. § 2702(b)(3) (2006).

135. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 900 (9th Cir. 2008), *rev'd on other grounds sub nom.*, City of Ontario v. Quon, 130 S.Ct. 2619 (2010). On the other hand, the Ninth Circuit has since concluded that opened messages on the Facebook and MySpace messaging services are held in remote computer service. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

A warrant is required for disclosure to authorities by a provider of "electronic storage" of the contents of a communication "in electronic storage" in a wire or "electronic communications system" for less than 181 days.[136] A subpoena or court order will suffice after 180 days or when authorities seek content disclosure from a provider of "remote computing service" of a communication "held or maintained on that service – (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission), a subscriber or customer of such remote computing service; and (B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."[137]

One court has concluded that a web-based e-mail provider must comply with a criminal trial subpoena for the contents of a subscriber's opened e-mail even though it had been stored with the provider for less than 181 days.[138] The district court determined that the e-mail was not in the type of "electronic storage" that would have triggered the application of section 2703(a)'s warrant requirement. The court reasoned that the e-mail of web-based users is not in electronic storage because it does not fit the "backup" requirements of 2510(17)(B). From the court's perspective, the backup reflects the practice of non web-based e-mail users who download their e-mail to their own computers and only leave their e-mail with their service provider as backup. Web-based e-mail users may store their e-mail with their providers, but since they ordinarily do not download them such storage cannot be considered backup.[139]

The SCA makes it more difficult for the federal government to access Facebook and MySpace communications. Private litigants were unsuccessful when they sought to acquire webmail and private messaging from Facebook and MySpace in *Crispin v. Christian Audigier, Inc.*[140] The litigants argued that the subscribers whose communications were at issue had no standing.[141] Nor could they convince the court that section 2703(e), which immunizes providers from compliance with court orders and subpoenas, contemplated private party

136. 18 U.S.C. § 2703(a) (2006).

137. 18 U.S.C. § 2703(b) (2006).

138. United States v. Weaver, 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009).

139. *Id.* at 772 ("Thus, unless a Hotmail user varies from default use, the remote computing service is the only place he or she stores messages, and Microsoft is not storing that user's opened messages for backup purposes. Instead Microsoft is maintaining the messages 'solely for the purpose of providing storage . . . services to such subscriber or customer.' 18 U.S.C. §2703(b)(2)").

140. *Crispin*, 717 F. Supp. 2d, at 965.

141. *Id.* (citing J.T. Shannon Lumber Co. v. Gilco Lumber, Inc., No. 2:07-CV-119, 2008 WL 3833216 (N.D. Miss. Aug. 14, 2008)).

access to provider-held customer communications.[142]

Federal officials may secure electronic communications service or remote computing service customer-related transaction information (name, address, means of payment, etc.) under an administrative subpoena without the necessity of notifying the customer.[143] If an ISP is served a search warrant for electronic communications content, pursuant to 18 U.S.C. § 2703(a) the service provider must comply with Rule 41 of the Federal Rules of Criminal Procedure, which includes providing a copy of the warrant and receipt for any property seized to the service provider as required by Rule 41(f)(1)(C).[144] Neither SCA nor the Fourth Amendment, however, requires them to notify the person to whose communication they have access.[145]

Like the ECPA, the SCA should contain additional provisions that permit more information sharing between the private sector and the government in context of national security. The need for severe sanctions for abusing this information sharing should be balanced as to not chill the relationship between the government and private sector in the information sharing arena. "Lack of statutory clarity [may cause] judicial uncertainty,"[146] but it may also prevent the national security community from accessing threat information that could interrupt an attack against Americans or American interests. Because courts are increasingly denying government requests for retrospective geolocation data without a warrant (citing the SCA),[147] statutory amendments must include the authority for the national security community to access this information.

142. *Crispin*, 717 F. Supp. 2d, at 965.

143. 18 U.S.C. § 2703(c)(2)-(3) (2006); United States v. Cray, 673 F. Supp. 2d 1368, 1378-79 (S.D. Ga. 2009) (citing United States v. Bobb, 577 F.3d 1366, 1368 n.1 (11th Cir. 2009)).

144. *In re* Application of the U.S., 665 F. Supp. 2d 1210, 1215-21 (D. Or. 2009) (citing *In re* Search of Yahoo, Inc., No. 07-3194-MB, 2007 WL 1539971, *6 (D. Ariz. May 21, 2007)); United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008); *In re* Search Warrant, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032, *5 (M.D. Fla. Feb. 13, 2006). *But see* United States v. Kernell, No. 3:08-CR-142, 2010 WL 1408437 (E.D. Tenn. Apr. 2, 2010) (holding that search warrants issued for provider-held evidence under section 2703 enjoy extraterritorial vitality notwithstanding apparent language to the contrary in Rule 41(b)).

145. *In re* Application of the U.S., 665 F. Supp. 2d at 1221-24.

146. Burr, *supra* note 90, at 11.

147. *Id*. at n.64 (citing *In re* the Application of the U.S. for an Order Directing the Provider of Elec. Commc'ns Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585 (W.D. Pa. 2008), *vacated*, 620 F.3d 304 (3d Cir. 2010) ("Government's requests for Court Orders mandating a cell phone service provider's covert disclosure of individual subscribers' (and possibly others') physical location information must be accompanied by a showing of probable cause.").

3. The Gaps in the Foreign Intelligence Surveillance Act

The Foreign Intelligence Surveillance Act of 1978[148] established a "statutory procedure authorizing the use of electronic surveillance in the United States for foreign intelligence purposes."[149] Amended many times since passage, FISA governs most national security electronic surveillance. Its threshold requirement is "probable cause to believe that 'the target of the electronic surveillance is a foreign power or agent of a foreign power.'"[150] Even in its amended form, FISA hinders national security investigations.

FISA has been outpaced by technology. According to Benjamin Wittes, "the communications and data infrastructure FISA sought to regulate no longer exists . . . ."[151] Current cyber security threats require access to data from cyberspace with appropriate executive, legislative, and judicial oversight mechanisms. Electronic surveillance law must recognize that in the world of social networking, instant messages, and packetized data streams, state boundaries are meaningless. Rather than being geographically focused, surveillance law needs to be at least as concerned with how data is used as it is about "how easily [the] government can collect it in the first place."[152]

FISA's standards for access by the government to electronic communications are much more demanding than those under the SCA.[153] The few publicly available FISA decisions indicate that litigation may arise under sections 1806(f) and 1825(g) that allow for limited challenges to the exercise of FISA authority in the context of electronic surveillance and physical searches.[154]

148. 50 U.S.C. §§ 1801-1862 (2006).

149. H.R. Rep. No. 95-1283, at 22 (1978).

150. Baker, *supra* note 36, at 80 (quoting 50 U.S.C. § 1804(a)(4)(A)).

151. WITTES, *supra* note 14, at 222. These technology changes are outlined in LTG Keith Alexander's responses to questions posed at a Senate hearing FISA for the 21st Century available at http://www.fas.org/irp/congress/2006_hr/alexander-qfr.pdf ("When FISA was enacted into law in 1978, almost all transoceanic communications into and out of the United States were carried by satellite and those communications were, for the most part, intentionally omitted from the scope of FISA, consistent with FISA's focus upon regulating the collection of foreign intelligence from domestic communications of United States persons. Congress could not have anticipated the revolution in telecommunications technology that would establish global, high-speed, fiber-optic networks that would fundamentally alter how communications are transmitted. Nor could Congress have anticipated the stunning innovations in wireless technology, or the explosion of the volume of communications, that have occurred in recent decades. Unpredicted advances in the development and deployment of new technologies, rather than a considered judgment by Congress, has resulted in the considerable expansion of the reach of FISA to additional technologies and communications beyond the statute's original focus on domestic communications.").

152. *Id.* at 231.

153. *See generally* 50 U.S.C. § 1812 (2006).

154. Two of the recent decisions, concerning challenges to the National Security Agency's purported Terrorist Screening Program, group section 1845 with sections 1806 and

After the Terrorist Surveillance Program was disclosed in 2006, the Electronic Frontier Foundation sued AT&T for assisting NSA with the surveillance of AT&T customers.[155] There was strong debate in the U.S. Senate about new FISA legislation that granted "retroactive immunity to telecommunications companies that assisted the NSA in warrantless surveillance of Americans."[156] Some senators argued that "telecommunications companies should not be punished for assisting the government in its fight against terrorism."[157] Others argued that the bill rewarded telecommunications companies for violating the law and betraying the privacy of their customers. Despite dissent, the bill passed and President Bush signed the FISA Amendments Act of 2008 into law on July 10, 2008.[158]

The FISA, even in its amended form, has already hindered counterterrorism network surveillance.[159] An important addition to FISA under this Act was its expansion of FISA's coverage to include surveillance of Americans living overseas. Under § 702(b) of FISA, the government may not "intentionally target a United States person reasonably believed to be located outside the United States."[160] Previously there was no procedure for obtaining a warrant for surveillance of Americans overseas because magistrate judges had no extraterritorial jurisdiction under the Federal Rules of Criminal Procedure.[161] "By placing Americans overseas under FISA, Congress created a procedure for protecting the privacy of all Americans subject to foreign intelligence surveillance."[162] In addition, Section 702 outlines the procedures for targeting non-U.S. citizens outside the United States.[163] It includes a provision that prohibits the intentional electronic surveillance of "any person

1825 in their rejection of the defendant's sovereign immunity argument. *In re* Nat'l Sec. Agency Telecomm. Records Litig., 700 F. Supp. 2d 1182, 1192 (N.D. Cal. 2010) ("But FISA directs its prohibitions to 'Federal officers and employees' (see, eg, 50 U.S.C. §§1806, 1825, 1845) and it is only such officers and employees acting in their official capacities that would engage in surveillance of the type contemplated by FISA.") (quoting *In re* Nat'l Sec. Agency Telecomm. Records Litig., 564 F. Supp. 2d 1109, 1125 (N.D. Cal. 2008)).

155. John Markoff & Scott Shane, *Documents Show Link Between AT&T and Agency in Eavesdropping Case*, N.Y. TIMES, Apr. 13, 2006, at A17.

156. Jonathan D. Forgang, *"The Right of the People": The NSA, The FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas*, 237 FORDHAM L. REV. 78, 237 (2009).

157. *Id.*

158. Eric Lichtblau, *Senate Approves Bill to Broaden Wiretap Powers*, N.Y. TIMES, July 10, 2008, at A1.

159. *Surveillance and Shahzad: Are Wiretap Limits Making it Harder to Discover and Pre-empt Jihadists?* WALL ST. J., May 13, 2010, at A13.

160. 50 U.S.C. § 1881a(b)(3) (2006).

161. FED. R. CRIM. P. 41(b); *see also* United States v. Bin Laden, 126 F. Supp. 2d 264, 275-76 n.13 (S.D.N.Y. 2000) (stating that there is not a statutory provision for searches conducted overseas), *aff'd sub nom. In re* Terrorist Bombings of U.S. Embassies in E. Afr. (Fourth Amendment Challenges), 552 F.3d 157 (2d Cir. 2008).

162. Forgang, *supra* note 156, at 238.

163. 50 U.S.C. § 1881a.

known at the time of acquisition to be located in the United States."[164] This means that the collection of a terrorist target must stop when and if the government discovers that the target of surveillance has landed in the United States.

Section 703 outlines the Foreign Intelligence Surveillance Court's authority for approving the surveillance of U.S. persons outside the United States.[165] It states:

> The Foreign Intelligence Surveillance Court shall have jurisdiction to review an application and to enter an order approving the targeting of a United States person reasonably believed to be located outside the United States to acquire foreign intelligence information, if the acquisition constitutes electronic surveillance or the acquisition of stored electronic communications or stored electronic data that requires an order under this Act, and such acquisition is conducted within the United States.
>
> *If a United States person targeted under this subsection is reasonably believed to be located in the United States during the effective period of an order issued pursuant to subsection (c), an acquisition targeting such United States person under this section shall cease unless the targeted United States person is again reasonably believed to be located outside the United States while an order issued pursuant to subsection (c) is in effect.* Nothing in this section shall be construed to limit the authority of the Government to seek an order or authorization under, or otherwise engage in any activity that is authorized under, any other title of this Act.[166]

This section emphasizes that electronic surveillance must stop when the government recognized that the target is inside the United States.

Until recently, these protections seemed reasonable in accordance with the Fourth Amendment and to have little effect on the electronic surveillance of terrorist targets. The growing number of U.S. citizens or dual citizenship terrorists has changed this calculus. With U.S. persons now recognized as potential terrorists, electronic surveillance laws such as the FISA must adapt to allow the access of computer network communications such as e-mails and instant messages to be collected. Under the current regime, electronic surveillance of any target must stop once the government recognizes the target is in the United States. Furthermore, if the target is recognized as a U.S. citizen that collection must stop until the intelligence community obtains approval from the Foreign Intelligence Surveillance Court.

The FISA must be adjusted to accommodate for the U.S. citizen terrorist and to close the gap between section 702 and FISA Title I collection. There must be amended FISA language that accommodates the transfer of collection from authorities found under section 702 and those under FISA Title I.

---

164. 50 U.S.C. § 1881a(b)(1) (2006).

165. In 1990, the Supreme Court held in *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990) that non-U.S. citizens living in another country and searched by the American government are not entitled to the protections of the U.S. Constitution.

166. 50 U.S.C. § 1881b(a)(1)-(2) (2006) (emphasis added).

In 2000, future Director of National Intelligence Mike McConnell said that "New thinking is required . . . to harness [signals intelligence] capabilities to control vulnerabilities of the information age."[167] McConnell was prescient in describing the challenges now shared between the National Security Agency and U.S. Cyber Command:

> No other government agency, now or in the foreseeable future, will match NSA's ability to detect and react to an information attack. This point is controversial because today cyber penetrations are no longer hindered by traditional borders, and it is increasingly difficult to distinguish between foreign and domestic threats; yet, NSA's capabilities are limited to use against only foreign targets. Now that telecommunications and networking have eliminated many of the traditional boundaries that protected the United States from foreign influence and activity, we need to think differently about how to use and develop NSA's capabilities.[168]

The FISA is an important capability used by the national security community. Malicious activity in cyberspace is difficult to classify as a "foreign nation state [attack] – an intelligence and defense or national security event, a domestic attack – a law enforcement concern – or an attack by a terrorist group – a law enforcement concern as well as an intelligence and defense or national security event."[169] Modern electronic surveillance authorities must incorporate this reality and enable the power of the national security community to be applied in a manner that is effective and effectively overseen.

CONCLUSION

Laws intended to govern domestic electronic surveillance now have an adverse impact on national security activities because they influence how cooperative the information service providers can be with the national security community. Laws such as the Electronic Communications Privacy Act and the stored Communications Act may create criminal and civil liabilities for the private sector that eliminate their motivation to assist in issues of national security. These laws provide needed protections for the privacy of ISP customers, but amendments must be made to allow the sharing of network security and threat information with the government.

The FISA attempts to govern electronic surveillance in the national security context, but the law has been outpaced by technology and compromised by terrorists who are also U.S. citizens. The law must be amended to permit seamless collection against threats to homeland security. The law can be amended in accordance with the content/non-content regime

167. J.M. McConnell, *The Future of SIGINT: Opportunities and Challenges in the Information Age*, DEF. INTELLIGENCE J., Summer 2000, at 40.

168. *Id.*

169. *Id.* at 46.

advocated by Professor Orin Kerr:

> The same principles should allow particularity for Internet searches that specify a particular individual rather than a specific Internet account. In the Internet setting, there are two different kinds of evidence collection: real-time wiretapping, which would be done under the Wiretap Act, and access to stored materials, done pursuant to the Stored Communications Act.[170]

Electronic surveillance law has evolved at a slower pace than electronic communications technology. In the digital age, given our digital dependence, we must amend the regulation of government electronic surveillance to better defend against current cyber threats.

170. 18 U.S.C. §§ 2701-2711 (2006).