NATIONAL SECURITY ON THE LINE

SUSAN LANDAU*

INTRODUCTION[1]

Wiretaps have been used by United States law enforcement for well over a century.[2] However, with the exception of a brief period during the First World War,[3] not until the 1960s did Congress pass the first federal statute governing their use. Title III of the 1968 Omnibus Crime Control and Safe Streets Act,[4] which regulated the use of wiretaps in criminal investigations, was followed by the 1978 Foreign Intelligence

* Susan Landau, Distinguished Engineer, Sun Microsystems. Email: susan.landau@sun.com. My work on this article has greatly benefited from the comments of Yochai Benkler, Whitfield Diffie, Michael Froomkin, Marc Rotenberg, and Roland Trope.

1. This article is based on Susan Landau, *Security, Wiretapping, and the Internet*, IEEE SECURITY AND PRIVACY, 26-33 (Nov./Dec. 2005). 2005 IEEE.

2. SAMUEL DASH, THE EAVESDROPPERS 23 (1959).

3. The Anti-Wiretap Statute (40 Stat. 1017, 1918) was in effect during the latter part of the war to prevent enemy agents from wiretapping.

4. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2521 (1968).

Surveillance Act,[5] which regulated the use of wiretaps in foreign-intelligence investigations. As telecommunications technology changed, law enforcement sought to keep the law current, and the Electronic Communications Privacy Act[6] and the controversial Communications Assistance for Law Enforcement Act (CALEA)[7] were passed.

In requiring that digitally-switched telephone networks be designed in accordance with federally-specified wiretapping standards, CALEA substantively changed the way telecommunications equipment was developed and deployed. Disagreements between the telephone companies and the Federal Bureau of Investigation (FBI), which had been charged with developing the CALEA standards, made implementation of the 1994 law exceptionally difficult. As a result, the Federal Communications Commission (FCC) delayed required implementation two years.

In 2004, the FBI petitioned the FCC to extend CALEA to Voice over IP (VoIP), meaning voice communications over the Internet (or using Internet protocols). CALEA, which placed law enforcement in the middle of the design process of communications technology, represented a fundamental alteration in the wiretapping laws established by Title III and FISA, and the result has been a chaotic and difficult implementation process. Because of the different architectures of the telephone and Internet networks, implementing CALEA on VoIP is likely to be even more difficult than implementing CALEA on telephony networks.[8] It not only poses risks to the U.S. economy (the potential loss of corporate information), but also to the freedom of U.S. citizens, and to U.S. national security (through the enabling of cost-effective massive intelligence gathering). This article focuses on those threats posed to national security though the reader should be aware of other objections to the FBI proposal, including concerns about threats to innovation and to civil liberties.[9] The issue of CALEA and VoIP is not the first time that conflict has arisen between the needs of law enforcement and the interests of national security in communications

5. 50 U.S.C. § 1801 (2006).

6. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986).

7. Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (1994).

8. *See, e.g.,* IAB and IESG, RFC2804 — IETF Policy on Wiretapping (May 2000), http://www.rfc-archive.org/getrfc.php? rfc=2804.

9. *See, e.g.,* Joint Reply Comments of 8X8 Inc. et al., to the Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295 (Dec. 21, 2004), *available at* http://www.cdt.org/digi_tele/20041221joint.pdf; Joint Reply Comments of 8X8 Inc. et al., to the Communications Assistance for Law Enforcement Act and Broadband Access and Services, ET Docket No. 04-295 (Nov. 8, 2004), *available at* http://www.cdt.org/digi_tele/20041108indpubint.pdf.

infrastructure. In many ways, the fight over implementing CALEA in VoIP is reminiscent of the battles over the use of strong encryption during the 1990s, the "Crypto Wars."[10] Just as now, in the Crypto Wars, there were disputes about threats to innovation and civil liberties. Ultimately national security concerns, which include the need for good methods to ensure information security, carried the day. As a result, strong encryption is deployed throughout the infrastructure, despite the difficulties that the availability of strong encryption may pose for some national security and law enforcement investigations

CALEA requires building wiretapping capabilities into communications networks. The same issues are in play in CALEA applied to VoIP as existed in the Crypto Wars: although law enforcement has investigatory reasons for seeking to apply CALEA to VoIP, the national security requirements for information protection should be paramount. These argue against building an architected security breach into the communications network such as CALEA would require.

Understanding the issues raised when CALEA is applied to VoIP requires knowledge of a number of disparate areas. Part I traces the history of U.S. wiretap law, demonstrating what an abrupt change CALEA represents in wiretapping law. The problems that ensue when placing a law enforcement agency in charge of designing telephony standards are illustrated in Part II by tracing the history of CALEA. Indeed, the difficulties are compounded by applying CALEA to VoIP, because VoIP travels on a packet-switched network. Part III explains how the architecture of the Internet causes that network to be easier to subvert than circuit-switched networks. Through examining current reliance on the Internet as well as future dependencies created the by "billions and billions of devices" that will be connected to the Internet, Part IV presents the security threats that result from building surveillance tools into Internet communications protocols.

Investigating terrorist cases involve unusual techniques and require enrolling the "community." Part V analyzes the policy issues surrounding communications surveillance and terrorism investigations, and demonstrates that the law enforcement approach is counter-productive. The article concludes with an observation that CALEA, which forces surveillance capabilities into communications networks, represents a turnaround in U.S. policy of protection of communications privacy, a policy begun in the 1790s.

CALEA represents a sharp break with U.S. wiretap law. Its application to Voice over IP creates numerous security vulnerabilities.

10. *See, e.g.*, STEPHEN LEVY, CRYPTO: HOW THE CODE REBELS BEAT THE GOVERNMENT SAVING PRIVACY IN THE DIGITAL AGE (2001).

Security requirements should be, "First, do no harm." CALEA applied to VoIP does not pass this test and should not be approved.

I. FEDERAL WIRETAPPING LAWS: A SHORT HISTORY

In putting the FBI into the role of designing wiretapping standards,[11] CALEA altered previous wiretap law, which proscribed rules governing the "tapper."[12] A brief history of U.S. wiretap law illuminates how anomalous CALEA is.

Except for a brief time during the First World War,[13] the first federal wiretap law appeared in 1967, in response to the *Katz*[14] case. The Supreme Court has ruled warrantless electronic bugging[15] illegal, establishing the doctrine of "legitimate expectation of privacy."[16]

Charles Katz was a gambler. Through an electronic bug put on a Los Angeles public phone booth, law-enforcement agents recorded Katz placing bets, in violation of Federal statutes prohibiting interstate gambling.[17] The Court ruled the law-enforcement bugging illegal. The Court found there is an expectation of privacy from even so public a place as a phone booth, and the warrantless bugs violated Katz's privacy. If there was to be electronic surveillance, a procedure for obtaining warrants needed to be enacted, spurring Congress to take action to regulate electronic surveillance.

The ensuing debate on wiretapping occurred during a period of social turmoil. The civil rights protests brought thousands of (non-violent) marchers to Washington; the opposition to the Vietnam War was about to do the same. The 1960s also saw the assassination of several of America's prominent leaders: President Kennedy, Malcolm X, Martin Luther King, and Senator Robert Kennedy. Into this context came the

11. CALEA, §§ 103, 107, (N.B. The law specifies the Attorney General will determine the standards issues, but that was understood during negotiations on the bill to actually mean the F.B.I.).

12. 18 U.S.C. §2518(4)(e) (2000). "An order authorizing the interception . . . shall . . . direct that a provider of a wire or electronic communication service . . . shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception . . . ."

13. Concern about enemy agents led to the federal Anti-Wiretap Statute.

14. Katz v. United States, 389 U.S. 347 (1967).

15. An electronic bug is a concealed microphone that operates by sending the signal through radio waves to the receiver, while a wiretap is a similar device that is connected to a communications circuit, such as the telephone network or the Internet, with the transmission being intercepted through the communications circuit itself.

16. The Katz decision did not use the expression "legitimate expectation of privacy," but in Smith v. Maryland, 442 U.S. 735, 740 (1979), the Court described the decision that way writing, "[c]onsistently with *Katz*. . . the application of the Fourth Amendment depends on whether the person . . . can claim . . . a 'legitimate expectation of privacy' . . . ."

17. Katz, 389 U.S. at 348.

findings of the 1967 President's commission on organized crime.[18]

Organized crime – widespread crime controlled through a centralized organization – was largely ignored by U.S. law enforcement (especially the FBI) until it was made quite public by the combination of the accidental discovery in 1959 of a meeting of crime bosses in upstate New York[19] and the testimony in 1963 of organized crime member Joseph Valachi to a Senate committee. With the lawbreakers' reliance on "victimless" crimes and its corruption of local law enforcement, organized crime is particularly difficult to investigate. The President's commission concluded that wiretapping was needed to break the back of organized crime. But even amongst law enforcement, there was not universal agreement with the commission.

Attorney General Ramsey Clark had prohibited federal law-enforcement use of wiretaps. The Chief Judge of the US District Court in Northern Illinois had testified to Congress that wiretaps were the mark of lazy investigators.[20] In a 1961 survey, attorneys general from California, Delaware, Missouri and New Mexico opposed federal wiretapping law.[21] Even President Johnson spoke against wiretapping.[22]

As Justice Louis Brandeis observed in his famous dissent in *Olmstead*,[23]

> [w]hen the Fourth and Fifth Amendments were adopted, 'the form that evil had heretofore taken' had been necessarily simple. Force and violence were then the only means known to man by which a government could directly impel self-incrimination . . . . But 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in

18. President's Commissions on Law Enforcement, *The Challenge of Crime in a Free Society* (1967).

19. On November 15, 1957, a New York state patrolman in the "southern tier" of the state, near Pennsylvania, came upon a meeting of organized-crime bosses. The patrolman set up a roadblock, resulting in the identification of sixty-seven people. *See e.g.*, WHITFIELD DIFFIE AND SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION (1998) at 168-69.

20. "In every case I know of where wiretapping has been used, the case could have been made without the use of the wiretap. Wiretapping in my opinion is mainly a crutch or shortcut used by inefficient or lazy investigators." S. REP. NO. 99-1097, at 1495 (1968).

21. *Wiretapping and Eavesdropping Legislation: Hearings on S. 1086, S. 1221, S. 1495, and S. 1822 Before the Subcomm. On Constitutional Rights*, 87th Cong. 545, 547, 554, 560 (1961).

22. 26 CONG. Q. WKLY. 1842 (July 19, 1968).

23. Olmstead v. United States, 277 U.S. 438, 473-76 (1928) (Brandeis, J., dissenting).

> court of what is whispered in the closet . . . . 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 . . . As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping.[24]

Experience had already shown that, just as Justice Brandeis has predicted, wiretapping is a broad form of investigatory search. Congress was well aware that the FBI's warrantless wiretapping had extended to members of the government; from the Truman era through the Nixon presidency, the FBI had wiretapped on Supreme Court Justices, Congressional staff, and other members of the government.[25] Nonetheless the Omnibus Crime Control and Safe Streets Act of 1968,[26] Title III of which established the basic law for interceptions performed in criminal investigations, was made law.[27] Because of concern over the intrusiveness of electronic surveillance searches, Title III tightly controlled their use.

The presidential commission recommended that law-enforcement wiretapping be limited to investigations of serious crimes and that a wiretap warrant be obtained only after a set of stringent requirements were met. Congress established these controls over law-enforcement wiretapping, as well as a public reporting mechanism, the *Wiretap Report,* published annually by the Administrative Office of the U.S. Courts. Title III was limited to wiretap warrants for investigations of criminal cases – but criminal investigations are only part of the wiretapping equation.

After *Katz*, warrantless electronic surveillance continued to be used for what were characterized as domestic "national security" cases. Then in 1972, the Supreme Court, ruled that "the constitutional basis of the President's domestic security role . . . must be exercised in a manner compatible with the Fourth Amendment."[28] The Court invited Congress to rectify the situation by establishing procedures for national-security wiretaps. Because of Watergate,[29] the process took half-a-dozen years.

24. *Id.*

25. *See, i.e.*, ALEXANDER CHARNS, CLOAK AND GAVEL: FBI WIRETAPS, BUGS, INFORMERS, AND THE SUPREME COURT*,* 25 (1992); INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, FINAL REPORT, BOOK III, S. REP. NO. 94-755, at 309 (1976).

26. 18 U.S.C. §§ 2510–2521 (1968).

27. These include §§2516-2519 of Title III.

28. United States v. Dist. Ct., 407 U.S. 297, 320 (1972).

29. "Watergate" refers to the 1972 burglary of the Democratic Party National Committee

The third-rate burglary[30] that brought down the presidency revealed widespread political wiretapping under the guise of national security investigations. The involvement of many of the intelligence agencies in surveillance activities caused great concern. In January 1975, the Senate appointed an eleven-member special committee to determine the extent to which "illegal, improper, or unethical" intelligence activities were engaged in by government agencies.[31] Thus was created the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, more commonly known as the Church Committee after its chair, Senator Frank Church. The Church Committee uncovered decades of government surveillance of what should have been protected political activity. Beginning its study with 1936, the Church Committee worked its way through a forty-year history of surveillance of, among others, ordinary citizens engaged in political activity, Congressional staff, Federal judges, and political activists. Neither party nor any President was immune to the temptation of electronic surveillance – wiretaps and bugs – used for political purposes.

Harry Truman wiretapped the Washington lobbyist (and FDR confidant) Thomas Corcoran. John F. Kennedy, during negotiations with Congress about sugar tariffs, acceded to tapping of Congressional staff. Kennedy and Lyndon Johnson both allowed the FBI electronic surveillance of Martin Luther King, Jr. During the 1968 Presidential race, Johnson arranged for the wiretapping of his own Vice President, Hubert Humphrey. Richard Nixon had tapped members of his staff, former members of his staff, the press, his political opposition, and ordinary citizens engaged in protected First Amendment activities.

The hearings revealed numerous illegal covert operations by the intelligence agencies, and the Church Committee concluded with a series of quite specific recommendations designed to protect the security and privacy of Americans:

o Recommendation 6: The CIA should not conduct electronic surveillance, unauthorized entry, or mail opening within the United States for any purpose.[32]

o Recommendation 15: NSA should take all practicable measures

offices at the Watergate complex in Washington by five men in the pay of the Republican Committee to Re-elect the President. Two years of investigations revealed extensive political spying and a cover up of the Watergate break-in by high government officials, including the President. President Nixon resigned, the first president ever to do so. *See, e.g.*, CARL BERNSTEIN AND BOB WOODWARD, ALL THE PRESIDENT'S MEN (1974).

30. This was how the Watergate break-in was originally characterized by Ron Ziegler, White House Press Secretary.

31. S. RES. 21, 94th Cong. (1975).

32. S. REP. NO. 94-755, at 302 (1976).

consistent with its foreign intelligence mission to eliminate or minimize the interception, selection, and monitoring of communications of Americans from the foreign communications.[33]

o Recommendation 16: NSA should not be permitted to select for monitoring any communication to, from, or about an American without his consent, except for the purpose of obtaining information about hostile foreign intelligence or terrorist activities, and then only if a warrant approving such monitoring is obtained in accordance with procedures similar to those contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[34]

o Recommendation 52: All non-consensual electronic surveillance should be conducted to judicial warrants issued under authority of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

The Act should be amended to provide, with respect to electronic surveillance of foreigners in the United States, that a warrant may issue if:

(a) There is probable cause that the target is an officer, employee, or conscious agent of a foreign power.

(b) The Attorney General has certified that the surveillance is likely to reveal information necessary to the protection of the nation against actual or potential attack or other hostile acts of force of a foreign power; to obtain foreign intelligence deemed essential to the security of the United States; or to protect national security information against hostile foreign intelligence activity.

(c) With respect to any such electronic surveillance, the judge should adopt procedures to minimize the acquisition and retention of non-foreign intelligence information about Americans.

(d) Such electronic surveillance should be exempt from the disclosure requirements of Title III of the 1968 Act as to foreigners generally and as to Americans if they are involved in hostile foreign intelligence activity (except where disclosure is called for in connection with the defense in the case of criminal prosecution.[35]

Based on the Church Committee's recommendations, the Foreign Intelligence Surveillance Act (FISA) became law in 1978.

Throughout this fifty-year history, from *Olmstead* to FISA, the central issue surrounding wiretapping was under what circumstances government agents would be permitted to wiretap. Title III and FISA struck a balance between law enforcement and civil liberties on electronic surveillance. Over the years, the balance has shifted some in the direction of law enforcement. First, the number of crimes subject to an

33. *Id.* at 309.
34. *Id.*
35. *Id.* at 327–28.

electronic surveillance order has gone from the original twenty-six in Title III to just under a hundred today.[36] Additionally, under the Electronic Communications Privacy Act,[37] pen registers and trap-and-trace devices, which record incoming and outgoing calls on a phone line, became obtainable under a subpoena.[38] Because the purpose of FISA was the collection of foreign intelligence, the requirements for an electronic surveillance order were looser than those of Title III, requiring only that the "target be a foreign power or an agent of a foreign power"[39] rather than the more restrictive "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense [enumerated elsewhere]."[40] For over two decades, FISA was limited to gathering foreign intelligence, but the Patriot Act changed the requirement on FISA from foreign intelligence being the "primary purpose" of the surveillance, to foreign intelligence being only a "significant purpose".[41] These changes, especially the diminution of the "wall" between Title III and FISA, are major ones, and have been the subject of serious discussion and analysis.[42]

Yet until CALEA, wiretap law did not delve into how the telephone networks should be configured. In each instance, wiretap law focused on what could be obtained and how law enforcement should obtain it (e.g., a subpoena in the case of a pen register or trap-and-trace order). In no instance prior to CALEA did Congress legislate how the communications providers should configure their networks; instead, Congress left the design of wiretap technology to the people who developed and ran the communications technology.

Leaving discretion about the architecture of the telephone network to the providers makes a great deal of sense. The telephone companies were required by law to satisfy the needs of law enforcement; at the same time, market forces make the privacy needs of their customers important to the company. So the telephone companies are in a natural position to balance the opposing needs of law enforcement and customer privacy. As a law enforcement agency situated in the executive branch, the FBI lacks a direct constituency that might demand protections for

36. James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 1 (1997), *available at* http://www.cdt.org/publications/lawreview/1997albany.shtml).

37. Pub. L. No. 99-508.

38. 18 U.S.C. §§ 3121-3127 (2001).

39. 18 U.S.C. § 1804 (2006).

40. 18 U.S.C. § 2518 (1998).

41. USA Patriot Act, 115 Stat. 272 (codified at 50 U.S.C. §1804(a)(7)(B).

42. *See, e.g.,* Daniel J. Solove, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & The USA Patriot Act: Surveillance Law: Reshaping the Framework: Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264 (2004).

communications privacy. By establishing the FBI[43] as the arbiter of the standards for wiretap-enabled digitally-switched telephony, CALEA eliminated the delicate balance that Title III and FISA had established between the competing needs of law enforcement and citizenry privacy rights.

With the advent of VoIP, the changes wrought by CALEA created not only privacy concerns but also security implications. CALEA requires an architected security breach in the communications network. The FBI's focus on solving cases and establishing a "chain of evidence" has caused the bureau to emphasize one set of issues—catching and convicting criminals —over another—securing U.S. communications. Indeed, CALEA requires an architected security breach in the communications network. The FBI's actions pursuant to CALEA impede the building of security protections into communications networks, an issue examined in the next section.

II. EXTENDING CALEA — WHAT DOES LAW ENFORCEMENT WANT?

The AT&T break-up in 1984 created a new problem for law enforcement: a large variety of service providers and equipment manufacturers. Instead of negotiating with a single provider on the standards for implementing legally authorized wiretaps, law enforcement faced a plethora of new telecommunications market participants.[44] In the early 1990s, the FBI began making public statements about law enforcement's inability to complete "hundreds" of surveillance orders.[45] In Congressional testimony, citing an "informal" 1993 survey of federal, state, and local law enforcement agencies, FBI Director Freeh stated there were 91 instances of electronic surveillance court orders that law enforcement could not implement due to technological impediments.[46]

43. CALEA establishes that the "Attorney General, in coordination with other Federal, State, and local law enforcement agencies" shall determine the standards; it was understood during negotiations on the bill that the FBI would be the actual agency determining the standards. 47 U.S.C. §1006(a)(1) (2006).

44. According to FBI testimony, by 1994 there were two thousand common carriers. Communications and Computer Surveillance, Privacy and Security: Hearing Before the Subcomm. on Technology, Environment and Aviation of the H. Comm. on Science, Space, and Technology, 103rd Cong. 5 (1994) (statement of James K. Kallstrom, Special Agent in Charge, Special Operations Division, New York Field Division, FBI).

45. "The development of technology is moving so rapidly that several hundred court orders already have been prevented by new technological impediments associated with advanced communications equipment." Louis Freeh, FBI Director, Address Before the American Law Institute (May 19, 1994), in CRYPTOGRAPHY AND PRIVACY SOURCEBOOK (David Banisar ed., 1994).

46. Network Wiretapping Capabilities: Hearing Before the Subcomm. on Telecomms. and Finance, H. Comm. on Energy and Commerce, 103rd Cong. 33 (1994) (testimony of Louis Freeh, FBI Director).

The public was not privy to the data leading to the conclusion that the nation's wiretapping laws needed an overhaul. When the survey information was finally made public in late 1994, the only data visible in the tables provided were the column headings and listings of the type of crimes being investigated[47] — everything else was blacked out. Without specific information about the difficulties law enforcement had encountered, it was impossible to determine how serious law enforcement wiretapping problems had actually been (and thus, by extension, the necessity for the new law). But that scarcely mattered: CALEA had already been enacted. Difficulties in its implementation were just beginning.

CALEA provided a "safe-harbor" provision, under which carriers that followed accepted industry standards would be considered in compliance with the law even if these carriers were actually unable to execute certain wiretaps.[48] There was, however, sharp disagreement over what constituted "accepted industry standards." During negotiations over the bill, the telephone companies had understood that accepted industry standards would be worked out jointly between industry and law enforcement, but after the law's passage, the FBI took the stance that it was in charge of setting these standards, called the "punch-list."

Civil-liberties groups and the telephone companies strongly objected to several of the proposed standards.[49] The ensuing controversy created considerable delays in carrying out the provisions of the Act. In response, Representative Bob Barr proposed the *CALEA Implementation Amendments of 1998*,[50] which would have delayed implementation of CALEA until October 1, 2000. Instead, the FCC stepped in and delayed required CALEA compliance to June 30, 2000.[51]

Meanwhile, the United States Telecommunications Association filed suit over aspects of "accepted" industry standards. One issue was

47. Sensitive Electronic Surveillance Techniques: Survey of Problems Encountered in Conducting Authorized Electronic Surveillance as Reported by FBI Field Offices, in 1995 EPIC Cryptography and Privacy Sourcebook: Documents on Encryption Policy, Wiretapping, and Information Warfare B 1-11 (1995).

48. CALEA (codified at 47 U.S.C. § 1006(a)(2) (2006)).

49. The FBI originally proposed a surveillance capacity of thirty-thousand simultaneous intercepts (wiretaps, pen registers, and/or trap-and-trace devices) at a time when the annual total of surveillances was less than a quarter that number. Implementation of the Communications Assistance for Law Enforcement Act, 60 Fed. Reg. 199, 53643-53646 (Oct. 16, 1995). After great objections to the methodology used in arriving at this number, the FBI revised the capacity estimate using a different method that resulted in a requirement for the capacity of sixty-thousand simultaneous surveillances (or eight times the number of annual wiretaps, pen registers, and trap-and-trace devices in 1996). *See* Implications of Section 104 of the Communications Assistance for Law Enforcement Act, 62 Fed. Reg. 9, 192 (Jan. 14. 1997).

50. H.R. REP. NO. 105-3221 (1998).

51. CALEA's original compliance date was October 25, 1998

extraction of *post-cut-through dialed digit* extraction – those digits sent *after* the initial connection. In old telephony systems, such digits did not exist; if a person wanted to access their checking account, for example, they had to speak to a person. Thus, if law enforcement wanted to record this communication, because it was part of a telephone conversation, law enforcement needed a wiretap warrant. But new technology has changed things. In modern punch-dial telephony systems, there is no person at the bank end of the call. Instead, the customer navigates to her account information through an automated phone menu. The FBI argued that since there was no conversation, such data should not be subject to a wiretap warrant, but instead could be released through a subpoena. The service providers disagreed.

Another contentious issue was location information. With fixed telephony systems, location information had not been an issue, but cell phones created a novel situation. During the CALEA hearings, FBI Director Louis Freeh had said that FBI would *not* require that call-identifying information, defined as "dialing or signaling information that identifies the origin, direction, destination, and termination of each communication", include location information.[52] Indeed CALEA is explicit on this issue: "call-identifying information . . .does not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)."[53] However, once CALEA passed, the situation changed. The FBI included the location of the cellular antenna serving the call as part of the proposed CALEA standards for call-identifying information.

In *USTA v. FCC*, the D.C. Circuit affirmed a District Court ruling that the FCC incorrectly granted several of the FBI punch-list requirements.[54] Specifically, the court ruled that the post-cut-through digits could not be obtained solely through a pen-register subpoena, but instead required a wiretap order. However, the D.C. Circuit agreed with the FCC ruling that location of the cellular tower was to be disclosed

52. "[Call setup information] does not include any information which disclose the general location of a mobile facility or service, beyond that associated with the area code or exchange of the facility or service. There is no intent, whatsoever, with reference to this term, to acquire anything that could properly be called 'tracking information.'" *Digital Telephony and Law Enforcement Access Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary and the Subcommittee on Civil and Constitutional Rights of the House Committee on the Judiciary,* 103rd Cong. 6 (1994) (statement of Louis Freeh). "Call setup information" was later changed to the term "call-identifying information, and that is the expression used in the law.

53. CALEA §103(a)(2)(B) (codified at 47 U.S.C. §1002).

54. 227 F.3d 450 (D.C. Cir. 2000).

with call-identifying information.[55] This yielded a brief period of peace that was quickly beset by a new set of issues.

In late 2003, the FBI gave notice to the FCC that the CALEA requirements should be extended to VoIP. This demand was controversial. CALEA has an exemption for "information services," a reference to the (nascent) Internet of 1994. Specifically, CALEA exempts "information services" from the common carriage requirements applying to telecommunications carriers.[56]

In its March 2004 petition to the FCC, the FBI declared that the ability of law enforcement to wiretap "is *being compromised today*,"[57] and the movement of voice calls to the Internet is already threatening law enforcement's capabilities to conduct electronic surveillance.[58] Despite the sweeping statement of "the serious impact" of the move to packet-based networks, however, no concrete evidence of actual failures of wiretapping VoIP were presented.[59] Indeed, a recent Inspector General report on CALEA implementation says quite the contrary.[60]

The FBI claimed that there was an ambiguity in the meaning of "telecommunications service" and requested that the Commission clarify which services and entities are subject to CALEA.[61] The Bureau also requested that the Commission establish benchmarks and deadlines for

55. *Id.*

56. CALEA §102(8)(A)(B)(C) (codified at 47 U.S.C. §1001).

57. Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act, filed by the U.S. Department of Justice, the Federal Bureau of Investigation & the Drug Enforcement Administration, 8 (Mar.10, 2004).[hereinafter The Petition].

58. *Id.* at 27.

59. *Id.*

60. The Inspector General's report said that,

> The FBI provided a document entitled *FBI Investigative Technology Division CALEA Law Enforcement Case Examples* dated October 29. 2004. The document contained 23 examples of unsuccessful intercepts, none of which involved electronic surveillance for wireline intercepts. The 23 examples involved either wireless or Voice over Internet Protocol (VoIP), which seemed to be law enforcement's primary concern since a low percentage of wireline intercepts are conducted. In addition, we believe these examples are not necessarily indicative of technology that is negatively impacting law enforcement's ability to conduct electronic surveillance because the carriers identified in these examples have either implemented CALEA solutions or contracted with a trusted third party to administer its CALEA responsibilities.

U.S. DEPARTMENT OF JUSTICE, OFFICE OF THE INSPECTOR GENERAL, AUDIT DIVISION, THE IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT, AUDIT REPORT 06-13, xi. The report further noted, "Three of the case examples described unsuccessful VoIP intercepts . . . In our judgement, these examples are not necessarily indicative of emerging technology that is negatively impacting law enforcement's ability to conduct electronic surveillance." *Id.* at 48-49.

61. The Petition, *supra* note 57, at 5-9.

CALEA compliance for packet-mode technologies.[62] According to the petition, the issue was that "the industry standards-setting organizations did not agree with Law Enforcement's position that industry is required to provide the same level of capability for packet-mode technology as it does for circuit-mode technology."[63] There was, however, ample evidence that the service providers were indeed working with law enforcement to develop VoIP wiretapping standards.[64] The FBI's stance is that compliance to these standards is voluntary and thus not reliable.

Despite the problems with the FBI's interpretation of CALEA, and despite the lack of evidence of actual harm, the FCC supported the FBI's interpretation. In August 2005, the FCC announced that broadband Internet providers of VoIP must comply with CALEA.[65] This was followed by a statement of FCC policy: "To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement,"[66] which was acknowledged to be about making it illegal for Americans to use such VoIP providers as Skype and PGPfone unless the software complied with CALEA.[67]

The FBI's petition produced a strong response from the telecommunications and computer industries and civil liberties groups; many raised the important legal issue that CALEA specifically exempted information services. This issue, while quite important, is not the focus of this article; our attention is on the security consequences of applying

62. *Id.* at 34-40.

63. *Id.* at 34-35.

64. The industry-developed surveillance standards include the Cable VoIP Solution, the Wireline VoIP Solution, the UMTS/GPRS/GSM VoIP Solution. *See* http://www.askcalea.net/standards.html, a website maintained by the FBI.

65. The actual rule appeared in 70 Fed. Reg. 197, 59664 (Oct. 13, 2005).

66. *In re Appropriate Framework for Broadband Access to the Internet over Wireless Facilities,* CC Dkt. No. 02-33 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf*; Review of Regulatory Requirements for Incumbent LEC Broadband Telecommunications Services,* CC Dkt. No. 01-337 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf*; Computer III Further Remand Proceedings: Bell Operating Company Provision of Enhanced Services; 1998 Biennial Regulatory Review —– Review of Computer III and ONA Safeguards and Requirements,* CC Dkt. Nos. 95-20 & 98-10 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf*; Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities,* CC Dkt. No. 00-185 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf*; Internet Over Cable Declaratory Ruling; Appropriate Regulatory Treatment for Broadband Access to the Internet Over Cable Facilities,* CS Dkt. No. 02-52 (Sept. 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf *;* POLICY STATEMENT*,* FCC 05-151 3 (September 23, 2005), *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

67. Declan McCullagh, *FBI to get veto power over PC software?*, News.Com (Sept. 27, 2005), http://news.com.com/2061-108043-5884130.html.

CALEA-type laws to VoIP, rather than the specific applicability of CALEA to VoIP.

The FBI's current focus is on packet-based communications technologies, which function rather differently than the circuit-switched telephone system. VoIP consists of routing voice conversations over the Internet or using Internet protocols. Voice is digitized, then broken into packets and sent over the Internet. The wide use to which packet-switched technology is being applied, and the differences between circuit-switched and packet-switched networks, mean that the application of wiretapping to information services is not straightforward. The next section explains how network-switching technology works, laying the groundwork for the later discussion of the dangers posed by applying CALEA to VoIP.

III. HOW DOES NETWORK-SWITCHING TECHNOLOGY WORK?

Although the public switched telephone network (PSTN) and the Internet are both communications networks, the architecture of the two networks is quite different. That difference has many consequences. A big difference is that the Internet is much simpler to subvert than the telephone network. To comprehend this difference, it is necessary to attain a basic understanding architecture in order to see the security difficulties that arise from applying CALEA to VoIP.

The PSTN is a circuit-switched network. When a call connection is created, the two parties[68] establish a direct path between them. For the duration of the call, only the two parties communicating use this path; it is a temporary, but dedicated, connection.

That picture is a bit of an oversimplification. In digitally-switched networks, it is possible to do "time division multiplexing." The data stream is divided into time slots; the temporary-but-dedicated connection is actually the time slot in the data stream, rather than the entire data stream.[69] That time slot is reserved even when the communicating ends are silent (and, of course, in a conversation typically one party is silent at any given time).

Callers connect through the *local exchange,* which is also known as the *central office.* Connections between the central offices are provided by a *tandem center,* which connects central offices that are not directly connected to each other. There is a hierarchy of such tandem offices, which serve increasingly larger areas.[70]

68. For the purposes of this paper, we will limit ourselves to communications between a pair of users, rather than considering multi-party communications.

69. ANDRÉ GIRARD, ROUTING AND DIMENSIONING IN CIRCUIT-SWITCHED NETWORKS 431 (1999).

70. UYLESS BLACK, COMPUTER NETWORKS: PROTOCOLS, NETWORKS, AND

The network routes calls through the cheapest available path. This is typically the shortest path, though it could be the one with the fewest number of switches, the least congestion, etc. Such routing reduces call delay.[71] Years ago, switches were mechanical objects physically connecting the wires that linked the callers. Now, of course, the switches are computers. The job of the computerized switches, however, remains much the same; the computer switches function as did the mechanical switches of old, albeit far more efficiently. In particular, the computer switches do not provide storage; the call comes in and goes out with no information stored at the switch.[72]

By contrast, the Internet is a "packet-switched" network. In such networks, fixed circuits are not dedicated for the duration of a communication. Instead, the data that is transmitted, whether files, email, Instant Messages, voice, is broken into small packets. Each packet travels its own route over the Internet. The entire set of contents is reassembled when it is received at the other end. The technology of packet routing creates some differences with circuit-switched technology.

In particular, the routes packets traverse is dynamically determined through addresses carried in the packets themselves. If a particular communication link is busy, the packet will be routed through a less-congested path. In theory — this occurs much less often in practice — each packet of a communication may travel a different route to its destination.

Another difference from circuit-switched technology occurs at the switches: the dynamic aspect of Internet routing means that it is a "store-and-forward" network; a switch waits to receive the entire packet contents before any of the packet bits are shipped out. Store-and-forward enables transmission in a network where nodes may be temporarily inaccessible. The bits of the packet sit at the switch before they are forwarded on. By contrast, none of the bits sit around at a telephone switch.

Although Voice over IP is a packet-switched technology, it has some different characteristics from other packet-switched applications such as file transfer and email. The most significant of these is that VoIP suffers serious quality-of-service problems if there is more than a 150 millisecond latency in packet delivery.[73] More precisely, VoIP must achieve the 150 millisecond bound in order to successfully emulate

INTERFACES 11-12 (1987).

71. *Id.* at 12-13.

72. *Id.* at 166.

73. U.S. DEP'T OF COMM., Special Pub. No. 800-58, D. Richard Kuhn et al., *Security Considerations for Voice over IP Systems: Recommendations of the National Institute of Standards and Technology* 19 (Jan. 2005).

current circuit-switched communications systems. This means that many of the standard security products, including firewalls,[74] network translation routers,[75] and virtual private networks,[76] all of which create latency by interposing additional functionality, are problems for VoIP.[77]

Wiretapping is performed somewhat differently on the two networks. A phone call may theoretically be wiretapped at any point along its path, although the most common place is at the frame — the set of racks at the local telephone exchange that place the incoming lines in numerical order.[78] Prior to the computer era, a tap was a physical object (just as was shown in all the old film noir). Modern switching technology, such as AT&T's ESS series and Northern Telecom's DMS-100, has simplified police wiretapping. Now the tap can be accomplished through the switch's ability to create conference calls. The tap is, after all, a conference call with a silent – and unacknowledged – third party.[79]

Wiretapping VoIP is simultaneously harder and easier than tapping a conventional phone call. On the one hand, because a telephone call always go through a central office, there is a natural place to tap circuit-switched calls. And because a telephone call uses a fixed circuit, a circuit-switched call is simpler to tap than a VoIP call, in which each packet route is dynamically generated. If one knows the IP address of the machine on which the VoIP call is being made —- this is the case for fixed devices (e.g., an office computer) —- then knowing where to place the wiretap on a VoIP call is easy. Otherwise it is not. The IP address, the Internet location of the computer on which the call is being made, may be one address when the user is calling from Starbucks at 3, another address using the free wireless lobby of the Hilton at 4, and still another from the airport lounge at 5. The changing nature of a user's IP addresses results in real complexity in placing a wiretap on the user's VoIP communications.

A variety of Internet security vulnerabilities make VoIP, which uses the packet-switched network, easy to intercept. The possibilities for

74. A firewall is a configuration of machines and software that prevents unauthorized users from accessing a computer network.

75. Network Address Translation boxes, or NATs, are devices, typically routers, that conform to an IETF standard enabling an endpoint to support more IP addresses than appear to the outside network. The NAT performs address translation to convert "public" addresses to "private" ones within the network.

76. Virtual Private Networks, or VPNs, are private networks configured within a public one, e.g., a corporation network running within the public Internet. Cryptography is often used to achieve confidentiality of the communications.

77. *See* Kuhn, *supra* note 73, at 19.

78. PATRICK FITZGERALD & MARK LEOPOLD, STRANGER ON THE LINE: THE SECRET HISTORY OF PHONE TAPPING 61-62 (1987).

79. DIFFIE & LANDAU, *supra* note 19.

interception include packet sniffers,[80] a web server interface for a VoIP switch or voice terminal, ARP cache poisoning[81] or flooding, etc. These possibilities for interception, however, do not necessarily simplify the problem for law enforcement.

The reason that the Internet is less secure than the PSTN is subtle. In essence it is because the Internet offers a much broader range of services. These services are sufficiently flexible that the Internet is able to make use of them in its own management. But the flexibility and dynamism of the Internet comes at a cost, namely the flexibility and dynamism make the Internet a much more difficult system to manage and secure. There are also other security differences between the two types of networks.

There are substantially different expectations regarding reliability of the two networks. Telephone networks are expected to have "five 9s" reliability, meaning that the network is available at least 99.999% of the year (which translates to under six minutes of outage annually). Few Internet-based systems are expected to be similarly reliable. Despite that, over the last two decades, modern societies have come to rely on two network communications systems: the circuit-switched telephony network, and the packet-switched Internet.

Thus, we are left with a set of complicated technological and policy issues. It is clear that for market and national security reasons, VoIP calls must enjoy the same privacy and security that circuit-switched telephony currently does. Yet in VoIP we have a technology that is more difficult to secure than traditional telephony. We also have a law-enforcement agency that would build security vulnerabilities into the communication protocols; these are issues we will explore in the next section.

IV. TECHNOLOGY RISKS POSED BY THE FBI'S PROPOSAL

Building surveillance technology into Internet communications protocols will create vulnerabilities. Some of the issues raised regarding

80. A packet sniffer is a hardware device or software program that monitors (passively intercepts) packets traversing a network.

81. Each device on a network has two addresses: a MAC (Media Access Control) address and an IP (Internet Protocol) address. The former is "permanent"; it resides on the physical network card inside the device, the latter is "dynamically" assigned, and can change if the device moves networks (or within the network). In order for information to be delivered to a device on the network, there needs to be a way to associate the MAC address with the IP address; this is the Address Resolution Protocol, or ARP. For efficiency's sake, the ARP information is kept in a cache, the ARP cache, so that it does not need to be looked up each time information has to go somewhere. "ARP cache poisoning" occurs when corrupt information is fed to the ARP cache, giving a false IP address to be associated with the MAC address.

the application of CALEA to VoIP are broader than technological security, e.g., the loss of U.S. competitiveness, while others are more narrowly focused. In this section, I discuss the technological problems raised by applying CALEA to VoIP.

A. The End-to-End Rule in Internet Architecture

The fundamental principle used in designing the PSTN was high quality for its most important application: voice transmission. The endpoints — the phone receivers — are dumb. In contrast, in the Internet, the intelligence is at the endpoints. The underlying network system is simple, leaving the endpoints able to deploy complex systems. The thought behind this design principle is that only the architects of the function in question would be in a position to fully understand what the application needed, and thus they should be the ones to provide it.[82]

The architectural idea of intelligence at the endpoints enables the Internet's versatility. Applications can be designed far beyond what the original designers of the Internet had in mind. Innovation has flourished because the simplicity of the Internet means that no one needs to depend on – or wait for – changes in the infrastructure in order to innovate. Thus applications as diverse as Google,[83] eBay,[84] and Skype[85] can be developed without changes to Internet infrastructure. The Internet's design flexibility comes at a price that we do not often think of as a price (we usually find it a benefit): the Internet is hard to control. This does not mean political or border controls (though those are also difficult to implement on the Internet), but design control. The flexibility afforded by the Internet to new applications means that there are few barriers to entry. The Internet boom of the late 1990s, seen by many as only the first step of the Internet revolution, was greatly facilitated by the low barrier to entry for new applications.

Marjory Blumenthal, Executive Director of the Computer Science and Telecommunications Board of the National Research Council from 1987-2003, and David Clark, one of the early Internet architects, and Chief Protocol Architect from 1981-1989, observed,

> When end points want to communicate, but some third party demands to interpose itself into the path without their agreement,

82. J.H. Saltzer et al., *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYSTEMS, 277, 278 (1984) ("The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communication system").

83. Google is currently the world's most popular search engine. *See* http://www.google.com.

84. Ebay is the originator of online auctions. *See* http://www.ebay.com.

85. Skype is a free Internet telephony service. *See* http:///www.skype.com.

> the end to end arguments do not provide an obvious framework to reason about this situation. We must abandon the end to end arguments, reject the demand of a third party because it does not 'fit' our technical design principles, or find another design approach that preserves the power of the end to end arguments as much as possible.[86]

Wiretapping is such an interposition. Building wiretapping capabilities into the Internet anywhere but the endpoints would require a fundamental change to Internet architecture. Thus applying CALEA to VoIP breaks the Internet's traditional end-to-end model.

Indeed, no longer would a small group of innovators be able to have an idea, develop it, and go to market; instead, early on, they would need to consult with the FBI. They would need lawyers and lobbyists — and time.[87] Such a process is hardly a useful way to encourage Internet innovation. The U.S. holds no lock on the ability to innovate. In the last decade, the Earth has become "flat"; research and development is burgeoning in China, India, and elsewhere.[88] Globalization, computing power, the Internet, and broadband have combined to enable business and research to flourish across the globe.

In threatening innovation, the FBI proposal not only poses problems for U.S. industry, but also for national security. Scientific and industrial strength were critical components of U.S. strength during both world wars and remain so today. A program that threatens domestic Internet innovation ultimately threatens national security.

B. The Internet and Critical Infrastructure

Complicating the national security issue, much of society's infrastructure now runs using Internet protocols. The Internet is an efficient and inexpensive communications medium, and the last decade has seen a massive shift to the Internet or to private networks using Internet protocols as the communications medium of choice. This shift was the result of millions of small decisions, and these were made even though the Internet protocols were insecure. There is no turning back.

This reliance on the Internet, and on Internet protocols, in turn raises concerns about the security of packet-switched networks, an issue explored by numerous recent government studies.[89] The control

86. Marjory Blumenthal & David Clark, *Rethinking the design of the Internet: The End to End Arguments vs the Brave New World*, 1 ACM TRANSACTIONS ON INTERNET TECH. 70, 73-74 (2001).

87. The recent FCC decision that VoIP must support E911 access presents many of the same threats to innovation.

88. *See generally* THOMAS L. FRIEDMAN, THE WORLD IS FLAT (2005).

89. *See e.g.*, JAMES ELLIS ET AL., PRESIDENT'S COMMISSION ON CRITICAL

infrastructure for various sectors, including electricity, water, and oil pipelines, uses a combination of private lines, leased lines, radio transmissions, and the Internet for communications. In recent years, in some cases the process control networks have been integrated with the business networks in order optimize dynamic pricing — e.g., raising and lowering the rates for electricity as capacity allows. But the business networks are, of course, connected to the Internet and thus that linkage leads to potential vulnerabilities. This threat is not merely theoretical.

Breaches have included a hacking incident into a telephone "loop carrier" switching system that disabled the Worcestor Airport's tower communications, shutting down the airport for six hours.[90] A similar attack on a sewage treatment plant in Maroochy Shire, Australia resulted in a release of thousands of gallons of untreated sewage into the local area.[91] The Slammer worm infected the Davis-Besse nuclear power plant, disabling a safety monitoring system (because the plant was shut off at the time, there was no immediate danger). The worm reached the plant through a machine on an unsecured network of a private contractor, thus bypassing the plant's firewall.[92]

Protecting critical infrastructure has taken on a new urgency. It is not just terrorists who are likely to target the networks supporting critical infrastructure; the Chinese government, for example, has "invested significantly in cyberwarfare training and technology,"[93] and Japan has already suffered a number of attacks originating in China and South Korea.[94] Cyberattacks on networks, especially in a vulnerable nation such as Taiwan, can have as destabilizing an effect as attacks on physical infrastructure.

Critical infrastructure information is not the only kind of private information that merits protection. Many types of corporate information, including those not directly dealing with critical

INFRASTRUCTURE, REPORT OF THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION (1997); PRESIDENT'S CRITICAL INFRASTRUCTURE PROTECTION BD., THE NATIONAL STRATEGY TO SECURE CYBERSPACE (Feb. 2003); UNITED STATES GENERAL ACCOUNTING OFFICE, REPORT TO THE COMMITTEE ON ENERGY AND COMMERCE, HOUSE OF REPRESENTATIVES, CRITICAL INFRASTRUCTURE PROTECTION: CHALLENGES FOR SELECTED AGENCIES AND SECTORS (2003).

90. Paul Festa, *DOJ Charges Youth in Hack Attacks*, News.Com, http: //news.com.com/2100-1023_3-209260.html (March 18, 1998).

91. Dana Shea, *Critical Infrastructure: Control Systems and the Terrorist Threat,* CRS REPORT FOR CONGRESS 7 (2003).

92. Kevin Poulsen, *Slammer Worm Crashed Ohio Nuke Plant*, The Register, http://www.theregister.co.uk/2003/08/20/slammer_worm_crashed_ohio_nuke/ (Aug. 20, 2003).

93. Robert Kaplan, *How We Would Fight China*, ATLANTIC MONTHLY, Jun. 2005, at 54, 55.

94. Anthony Faiola, *Anti-Japanese Hostilities Move to the Internet*, WASH. POST, May 10, 2005 at A12.

infrastructure information, need protection as well. For decades, U.S. companies have suffered from attacks on their unsecured communications systems. An incident from the 1970s illustrates the dangers that can result to the nation because of unprotected communications of private companies.

The Soviets had installed a major electronic eavesdropping center in the top floors of a house in Glen Cove, New York. The house was adjacent to Long Island Sound's "microwave alley," where much of the East Coast's communications traveled.[95] The Soviet equipment was capable of picking up conversations from a distance of one hundred miles. IBM was alerted that its corporate communications were not secure.[96] Nor were the communications of other companies. "[T]he Soviets could monitor all the telephone calls to and from the Department of Agriculture, and they ended up knowing more . . . than we did," a CIA veteran told the press.[97] That knowledge proved useful to the Soviets, who ended up buying up U.S. wheat at a favorable price. Meanwhile the U.S. ended up with a wheat shortage. Such incidents are not isolated to the 1970s. As recently as the 1990s, at least one U.S. manufacturer was warned by government officials that its microwave communications were vulnerable to eavesdropping.[98]

C. Network Architecture and Wiretapping

The layered[99] approach of Internet architecture does not preclude wiretapping. There is nothing inherent in the design of a communications network that precludes security or wiretapping, and indeed there are defense communications networks that simultaneously provide security and wiretapping capability. The Internet was originally designed as a resource-sharing network; neither security nor wiretapping were considerations in its initial design. While it is technically feasible to build an Internet that has intercept facilities with adequate security, it is unlikely to be politically or socially possible to do so now.[100]

95. William Broad, *Evading the Soviet Ear at Glen Cove*, 217 SCIENCE 910, 911 (1982).

96. KENNETH DAM ET AL., CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY 68 (1996).

97. Broad, *supra* note 95, at at 910.

98. DAM ET AL., *supra* note 96, at 68.

99. The Internet architecture is designed as a layered model, in which each layer uses the functions of the layer below. The seven layers are: physical, data link, network, transport, session, presentation, and application. The lower links are typically implemented in hardware, the upper ones, in software.

100. Fifteen years ago a transition to such a network might have been possible. If the U.S. government had sought, through a combination of R&D funding and other financial incentives to the ISPs, to create a secure Internet that enabled surveillance, it is possible that such a system could have been built. After all, at that time, the Internet was a U.S.

If laws or regulations were to require building access into Internet communications for U.S. law enforcement or national security, it is unlikely that such a protocol design could be accomplished securely. Building such requirements into managed networks (networks with central control) presents no serious technical difficulty. Building them into the peer-to-peer network that constitutes the Internet, however, does.

The Internet Engineering Task Force (IETF) creates the protocols that enable the Internet to work. These protocols must be carefully specified so that computers on the Internet can interoperate. In 2000 the IETF Network Working Group studied implanting wiretap requirements into Internet protocols. Their conclusion was that it could not be done securely.[101]

Such a conclusion stems from fundamental engineering principles. Complexity is the bane of security; additional program functionality increases the likelihood of a security breach.

D. The Threats are Real

By deliberately leaking information to a third party, wiretapping is an architected security breach. A recent hacking incident at Cisco illustrates the dangers of building wiretapping capabilities into the Internet.

Despite the IETF's reluctance to write wiretapping into network protocols, Cisco forged ahead, developing a proprietary architecture for VoIP interception at the router level. The interception would be performed by ISPs.[102] For this technology to function appropriately — and *not* deliver packets to unauthorized parties — the ISP network itself would need to be secure, a challenge for ISPs. Given that, it is ironic that Cisco was unsuccessful in protecting itself from a year-long Internet attack by a small group (possibly only a single individual) that succeeded in penetrating the router company and accessing protected information.[103] Despite notice of the repeated attacks, the company was

phenomenon and international cooperation was not required. That is not the case now. The Clipper lesson from a decade ago speaks loudly here. Foreign governments were simply not interested in a program in which the U.S. government held the encryption keys and so the U.S. found it impossible to arrange multi-lateral key-sharing agreements. There is no reason to suppose that such arrangements could be made now to enable a secure, surveillance-capable Internet.

101. Internet Architecture Bd. & Internet Eng'g Steering Group, IETF Policy on Wiretapping, RFC 2804 (2000), *available at* http://www.faqs.org/rfcs/rfc2804.html [hereinafter IETF POLICY ON WIRETAPPING].

102. FRED BAKER ET. AL., CISCO SYSTEMS, CISCO ARCHITECTURE FOR LAWFUL INTERCEPT IN IP NETWORKS, RFC 3924 (2004), *available at* http://www.faqs.org/rfcs/rfc3924.html.

103. John Markoff & Lowell Bergman, *Internet Attack Is Called Broad and Long*

nonetheless unable to prevent theft of proprietary software.

Building CALEA into VoIP would require security maintenance by the ISPs. Would ISPs be able to keep their "architected security breach" — the shipping of data to an authorized third party — fully secure? The ISPs, especially many of the smaller ones, are likely to be more vulnerable than Cisco.

Modern design paradigms make the problem worse. In the 1950s, if the NSA wanted copies of telegrams from the telecommunications companies, tapes with the telegrams were picked up by NSA courier.[104] The current model for tapping VoIP calls requires sending the bits via the Internet. Thus wiretapping is an architected security breach with the data automatically shipped remotely.[105] Enabling the remote delivery of data to a third party provides another potential for a security breach. In particular, the dangers posed by insider attacks continue to be much greater than the dangers posed by hackers. A rogue insider with the capability to conduct remote data delivery increases the likelihood that unauthorized surveillance will go undiscovered.

This is not a speculative threat. Recently, around one hundred mobile phones of members of the Greek government— including the prime minister—were illegally tapped for over a year.[106] This incident involved exactly the same architected security breach that wiretapping VoIP calls would require. Ericsson, a telecommunications supplier, had provided software to Vodafone that included "locked" eavesdropping capabilities. Someone at Vodafone subverted the system, activated the eavesdropping, and had the tapped communications delivered to a set of fourteen mobile phones. These events illustrate the potential for a rogue insider using the remote-management capabilities provided by a legally authorized eavesdropping system.

E. Enabling Surveillance by the Bad Guys

A technology designed to simplify Internet wiretapping by U.S. intelligence presents a fat target for foreign intelligence agencies. Breaking into this one service could yield broad access to Internet communications without the expense of building an extensive intercept

Lasting, N.Y. TIMES, May 10, 2005, at A1.

104. This was what was done during the "Shamrock" program, where tapes of all international telegrams from RCA Global, ITT World Communications, and Western Union International were shipped daily to the NSA.

105. This was the case, for example, with the FBI system for tapping email, Carnivore (now renamed DCS-1000).

106. *Spy Software Used in Mobile Eavesdropping*, KATHIMERINI ENGLISH EDITION, Feb. 3, 2006, *available at* http://www.ekathimerini.com/4dcgi/news/content.asp?aid=65958; Fotini Kalliri, *Wiretaps Kept Quiet for Eleven Months*, KATHIMERINI ENGLISH EDITION, Feb. 13, 2006, *available at* http://www.ekathimerini.com/4dcgi/news/content.asp?aid=66340.

network of their own.[107] Remote monitoring capabilities would mean that system vulnerabilities are thus as likely to be global as local. Were Internet wiretapping technology to be penetrated and exploited by foreign intelligence services, massive surveillance of U.S. "persons" (citizens and corporations) might follow.

There is another major infrastructure change that would further enable penetration and exploitation, namely the development over the last decade of very powerful search engines. Information that was public but was largely inaccessible, enabling security through obscurity[108] as it were, has now become trivial to discover and access. Internet wiretapping technology used in combination with inexpensive automated search technology could lead to an unprecedented compromise of U.S. security and privacy.

This problem is further aggravated by the direction of the Internet's development. Building surveillance capabilities into the Internet infrastructure, and not into the application endpoints, would expose to eavesdropping not only current applications but also future ones. Currently, there are millions of devices connected to the Internet, but we are rapidly moving to a situation of billions of resource-limited small devices such as radio-frequency identification (RFID) tags and sensors that will communicate via the Internet.

RFID tags are small devices with a computer chip and an antenna; they can receive and respond to radio-frequency queries from a transmitter. They are often the size of a barcode – a technology they will eventually replace – and they provide some of the same functionality, only more so. Cheaper RFID tags are passive, and only respond to a query, while more expensive tags have their own power sources that allow them to write on their tags as well as giving them longer ranges of broadcast. Tags respond to a signal from the reader and then transmit information, enabling functions like rapid authentication for entrance to secure facilities, product identification that enables tracking of goods, and the like. There is much more data on an RFID tag than a barcode, so that the RFID tag is able to identify not only the type of item – a Prada handbag – but the individual item itself – a Prada handbag sold at the Manhattan Saks Fifth Avenue on July 14, 2005. RFID tags will soon

107. Susan Landau, *Security, Wiretapping, and the Internet*, 3 IEEE SECURITY & PRIVACY 31, (Nov./Dec. 2005), *available at* http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/mags/sp/&toc=comp/mags/sp/2005/06/j6toc.xml&DOI=10.1109/MSP.2005.158.

108. The term "security through obscurity" is usually used to describe hiding security mechanisms in order to make them difficult to foil. Security through obscurity is viewed as a poor way of doing security, since what the methodology gains by secrecy is typically much less than what it loses through the lack of a public review. In the case I am describing here, the obscurity was accidental, an artifact of the previous difficulty of search.

be everywhere for use in inventory control, whether it be clothing or razor blades, for livestock tracking systems, for airline baggage handling, for logistics support for the Defense Department.

Sensor networks are networks that hook together small, inexpensive devices that measure such physical attributes as temperature, sound, and vibration. The sensors themselves have limited computing power and a limited energy supply. Sensors will be used in a myriad of remote monitoring scenarios, such as tracking environmental conditions or monitoring the state of elderly patients.[109] The devices themselves have limited memory, the networks have limited bandwidth, and there is also a lack of a priori knowledge of post-deployment configuration,[110] meaning the sensors do not know what the topology of the network is.

Neither RFID tags, which have been employed in the highway toll booth system for years, nor sensor networks, which were used during the Cold War to track the movement of Soviet submarines,[111] are new. What is new is the dropping cost of these technologies, which is enabling them to have a much wider range of uses. We are moving to a world of billions and billions of devices[112] that will be connected to the Internet.

Much of the data from RFID and sensor networks will remain in local area networks and not travel the Internet, but some types of data gathered will be aggregated in a central database. More to the point, the cheapness and ubiquity of the RFID and sensor technology means that even if a small percentage of these networks communicate via the Internet, this will provide a significant new and unprotected data source on the Internet. Both RFID tags and sensors are sufficiently small and low-powered that providing security is difficult. (Adequate security is, of course, dependent on context. The security needed to protect the data of an RFID tag on a razor on a Wal-Mart shelf is very different from the security needed to protect the data of an RFID tag on a diplomatic passport.)

F. We've Had This Battle Before

In 1996, the National Research Council released the report

109. For example, pulse-oximetry sensors would measure and report heart rate, rate of blood flow, and blood oxygen saturation.

110. Haowen Chan & Adrian Perrig, *Security and Privacy in Sensor Networks*, 36 COMPUTER 103, 103-05 (Oct. 2003), *available at* http://csdl2.computer.org/persagen/DLAbsToc.jsp?resourcePath=/dl/mags/co/&toc=comp/mags/co/2003/10/rxtoc.xml&DOI=10.1109/MC.2003.1236475.

111. The Sound Surveillance System (SOSUS) did this through hydrophones – long acoustic sensors – arrayed on the ocean floor.

112. The increase will also be fueled by portable personal communicating devices, e.g., cell phones and PDAs.

Cryptography's Role in Securing the Information Society.[113] The report's authors, among them a former deputy secretary of state, a former U.S. Attorney General, a former deputy director of the National Security Agency, and a former president of the Institute for Defense Analysis, concluded that, "[o]n balance, the advantages of more widespread use of cryptography outweigh the disadvantages."[114] Over the last several years, the government sought improvements in civilian communications infrastructure security, even though some of those improvements were likely to impede law enforcement investigations. The shift was clearly supported by the intelligence agencies, which found that the societal gains from increased information security outweighed the disadvantages to national security and law enforcement investigations. In addition, the military's move to save money by purchasing commercial off-the-shelf equipment meant that increases in the security of commercial equipment directly benefit defense agencies, enabling them to obtain the security they need without the necessity of producing custom products.[115]

The battle over applying CALEA to VoIP is in many ways reminiscent of the "Crypto Wars" of the 1990s. During that period, the FBI sought, through CALEA and the ill-fated Clipper key-escrow system, to hold on to its 1960s wiretapping capabilities in the face of advanced digital-switched telephony and other forms of digital communications. The Clipper program, announced in 1993, was a federal standard for protecting communications through an 80-bit cryptosystem and keys escrowed with agencies of the federal government. There were objections from industry and from civil liberties groups. In any case, international acceptance of the program, crucial for its success, never developed. As a result, the project was a dismal failure and few systems using it were ever built.[116]

In 2000, when U.S. national security agencies decided that the nation was better served through the deployment of strong cryptography,[117] support for the FBI position eroded and U.S. policy changed.[118] In part, the national security position changed because the

113. *See* Dam et al., *supra* note 96.

114. *Id.* at 6.

115. *See, e.g.*, Whitfield Diffie & Susan Landau, *The Export of Cryptography in the 20th Century and the 21st*, *in* SUN MICROSYS LABS: THE FIRST TEN YEARS 1991-2001, SUN LABS PERSPECTIVES ESSAY SERIES 410-15 (Jeanie Treichel & Mary Holzer eds., 2001), *available at* http://research.sun.com/techrep/Perspectives/PS-01-5.pdf.

116. *See id.* at 210-15.

117. This was not ever explicitly stated by the U.S. government, but the change to a more liberalized set of cryptographic export control rules would not have occurred without the support of the national security agencies.

118. The Department of Commerce, Bureau of Export Administration issued 15 C.F.R. Parts 734, 740, 742, 770, 772, and 742, Docket No. RIN: 0694-AC11, effective January 14, 2000. These would not have been issued without the strong support of the national-security

NSA and other agencies realized that the use of strong cryptography throughout the infrastructure – the protection of civilian information – was in many ways far more important than enabling law enforcement investigative techniques. In recent years, the government has encouraged a number of cryptographic efforts, including the development of the 128-bit Advanced Encryption Standard and the Elliptic Curve Cryptosystems.[119] Then, as now in the VoIP debate, the FBI pushed for the extension of wiretapping capabilities even though it could pose serious dangers to the protection of civilian information, including critical infrastructure.

A decade ago, Congress faced the dual issues of surveillance and communication security when it confronted CALEA and Clipper. Congress passed the wiretapping bill, but held a more jaundiced view of the key escrow program. A number of Senators and Representatives took positions against the Clipper chip.[120] In CALEA, Congress also explicitly excluded information services from the law's requirements. Congress' view was that wiretapping – and CALEA – makes sense for law enforcement in the PSTN environment, but issues of information security take precedence in the Internet environment.

At present, we are struggling to achieve adequate security in the Internet without intentional security compromises in its design. Although it may one day be possible to incorporate surveillance into packet-switched networks with sufficient security, it is hard to see how this could be less difficult than the unfinished task of developing scalable and economical secure networks. At the very least, built-in wiretapping would require secure communications of its own in order to carry the intercepted information to the customers for which it was being collected.

These changes do not mean that Internet communications cannot be wiretapped. The insecurity of the Internet is well known. Currently, few communications are routinely protected (e.g., encrypted end to end). As the IETF Network Working Group observed, "the use of existing network features, if deployed intelligently, provides extensive opportunities for wiretapping."[121] But exploiting current insecurities and

agencies.

119. *See* NIST Computer Sec. Div. Computer Sec. Res. Ctr. Focus Areas, http://csrc.nist.gov/focus_areas.html#csa.

120. In 1996 Senator Patrick Leahy introduced the Encrypted Communications Privacy Act of 1996 (S. 1587, 104th Cong. (1996)), which affirmed the right to use any form of encryption domestically. Meanwhile Senator Conrad Burns proposed a bill prohibiting mandatory key escrow and enshrining the freedom to sell and use any type of encryption domestically, and liberalized export rules. In the House, Representative Bob Goodlatte proposed a similar bill (H.R. 695, 105th Cong. (1997)). *See also* Diffie & Landau, *supra* note 115, at 222-23.

121. IETF POLICY ON WIRETAPPING, *supra* note 101.

actually building insecurities into Internet protocols have significantly different effects on the security of society's communications. I am arguing against the latter; I take no issue with the former.

V. SECURITY FROM A BROADER VIEWPOINT

The FBI is a law enforcement agency and it does what law enforcement agencies do: investigate crimes, arrest the perpetrators, and provide evidence for conviction. As a law enforcement agency, the FBI is committed to tools that can provide a "chain of evidence." This approach has proved successful in fighting organized crimes, drug dealers, and white collar crime. Law enforcement's view of what works in terrorist cases can be summed up by the 1991 statement of then FBI Director William Sessions: "[i]f a terrorist attack does occur, it is our view that a swift and effective investigation culminated by arrest, conviction and incarceration is a powerful deterrent to future acts of terrorism."[122] The evidence, including terrorists who were willing to fly airplanes into buildings in order to achieve their goals, would argue otherwise.

In the fight against violent fundamentalists, the FBI approach and tools are often inappropriate.[123] For example, given that the violent Islamic fundamentalist movement, has a potential base of millions, U.S. strategy must take into account that the war must be fought politically and economically, as well as militarily.

In earlier parts of this article, I argued that CALEA applied to VoIP is a poor security solution from a technological vantage point. In this section, I will show that ubiquitous surveillance technology proposed by the FBI is also a poor solution from a policy standpoint. I begin with putting various myths to rest.

We begin with the fact that September 11th was not the first instance of domestic terrorism in the United States. American history is replete with examples of homegrown terrorism, from Presidential assassinations, to racial terrorism exemplified by the Ku Klux Klan, to right-wing militias such as Posse Comitatus and the Order.

Nor is al Qaeda the first imported version of terrorism. Before the U.S. entry into the First World War, in an undeclared war, German saboteurs sought to cripple U.S. war production efforts. Though fewer

122. *FBI Programs: Hearing Before the Subcomm. on Civil and Constitutional Rights, Comm. on the Judiciary*, 102d Cong. 269-70 (1991) (statement of William Sessions, Director, FBI).

123. Violent Islamic fundamentalists are of greatest concern right now, but they are not the only religious zealots who have turned to violence; other examples include the rise of Hindu fundamentalism in India and the anti-abortion zealots who have turned to violence in the U.S.

lives were lost in terms of physical damage, the destruction was on a significantly greater scale than the destruction of the World Trade Center. The damage included the total destruction of a major munitions depot, blowing up over two million pounds of explosives, and many other acts of terrorism, including bombings of ships and chemical plants.[124]

Recent domestically-generated terrorism has included the Oklahoma City bombing and attacks on abortion clinics. These attacks, however, were neither on the scope nor scale of the attacks of September 11th, whose aftereffects include a radical reworking of U.S. domestic and foreign policy.[125] The National Commission on Terrorist Attacks upon the United States,[126] hereinafter referred to as the "9/11 Commission Report," observed that, "[t]he [terrorism] fostered by bin Laden and al Qaeda were on a scale approaching acts of war . . ."[127] Despite this, strategies to prevent terrorist attacks conform more closely to law enforcement practices than national security goals. There are a number of reasons for this.

One is psychological. There is simple comfort in viewing Islamic terrorism as criminal acts; "[if] bin Laden is a criminal whose activities are fueled by money – not a devout Muslim soldier fueled by faith – . . . Americans know how to beat well-heeled gangsters."[128] From the sheriffs in the Wild West, to the FBI ridding Chicago of its gangsters in the 1930s, the U.S. has a powerful mythology of the good guys always getting their man. The nation does not always win wars, but in U.S. lore, the sheriff walking down Main Street and the G-men in the dark alleyway always prevail.

A second powerful reason for the law enforcement approach is some

124. Black Tom Island, a munitions storage depot in New York Harbor, was blown up on July 30, 1916. The explosions destroyed windows in nearby Jersey City, as well as in Manhattan and Brooklyn; blasts were heard in Philadelphia (a hundred miles away). A total of over two million pounds of explosives were destroyed. Six-and-a-half months later, the huge shell-assembling plant of the Canadian Car and Foundry Company in Kingsland, New Jersey, which was building weaponry for Russia, was completely destroyed in a deliberately-set fire. The cost: seventeen million dollars. HENRY LANDAU, THE ENEMY WITHIN: THE INSIDE STORY OF GERMAN SABOTAGE IN AMERICA 77-91 (1937). In all, including fires and explosions in factories and in ships, German saboteurs caused over one hundred and fifty million dollars in damage to essential war goods. *Id.*

125. The controversial USA Patriot Act, as well as various regulations regarding air transportation initiated by the Transportation Security Administration, are one set of examples; another is the creation of the Department of Homeland Security; a third, and perhaps the most significant, are the two foreign wars fought since September 11th, in Afghanistan and in Iraq.

126. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S. (Comm. Print 2004).

127. *Id.* at 348.

128. MICHAEL SCHEUER (PUBLISHED AS ANONYMOUS), IMPERIAL HUBRIS: WHY THE WEST IS LOSING THE WAR ON TERROR 348 (2004).

early successes in the "war" on terror. The FBI's investigations of the PanAm plane crash over Lockerbie, Scotland and the first World Trade Center bombing led the public and policymakers to believe that the tools of law enforcement were the appropriate ones with which to combat terrorism.[129] These "missions accomplished" led to an aura of invincibility around law enforcement's capability to conduct the war on terror, an invincibility that continues to permeate the current discussions (which continue to center on there being no, as opposed to few, acts of terrorism occurring in the United States).

What drives law enforcement efforts is conviction in a court of law, but this is a misguided viewpoint. Anti-terrorism efforts could suffer under this type of mindset, because, as former U.S. Deputy Attorney General Philip Heymann has observed, in many cases law enforcement is not a deterrent to terrorists.[130] Violent Islamic fundamentalists often view a jail sentence as a form of martyrdom. Jail also provides an excellent opportunity for recruiting – sometimes amongst the nationals in the country in which the terrorism is to take place.

With its appropriate emphasis on proof, law enforcement investigations seek a level of evidence that will convict. This is not always an appropriate measure in a war against terrorists. As a CIA agent describes the situation,

> "Americans . . .ought also pray that Washington puts away the badge and warrant, and . . .U.S. and Western analytic corps and militaries . . .pull their weight against Al Qaeda by deciding this is a military, not a criminal foe . . .Al Qaeda can never be beaten while the U.S. attack is conceived and executed as an international version of the saga of the American West, where U.S. intelligence officers andsoldiers are sent out, like the storied Texas Rangers, and expected to always get their man."[131]

In spite of Constitutional and jurisprudential requirements of high levels of proof, such a law enforcement approach to terrorism has already incurred significant costs.[132] In contrast, the national security approach to cybersecurity is one of prevention. Currently, one area of national

129. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *supra* note 126, at 72.

130. PHILIP HEYMANN, TERRORISM AND AMERICA: A COMMONSENSE STRATEGY FOR A DEMOCRATIC SOCIETY 79 (MIT Press 1998).

131. *Id.* at 69.

132. During the Clinton administration, for example, law enforcement impeded U.S. government attempts to capture Osama bin Laden. Although this was an accident of the approach, rather than a deliberate impedance, the effect was real. *See* STEPHEN COLL, GHOST WARS: THE SECRET HISTORY OF THE CIA, AFGHANISTAN, AND BIN LADEN, FROM THE SOVIET INVASION TO SEPTEMBER 10, 2001 425-26, 495 (2004).

concern is the protection of critical infrastructure, much of which uses the poorly-secured Internet for communication; these include the electric power grid, the financial industry, transportation, telecommunications, and the health-care industry. In recent years, critical infrastructure protection has been the subject of a number of Presidential initiatives and is a major focus of the Department of Homeland Security.[133]

The better approach is a blend of the law enforcement and national security strategies. National security on its own can no more solve the terrorist problem than law enforcement can; what we must do is use each approach as it is appropriate to the situation. The desire to knock down the door, arrest the suspect, and go on to the next case should not take precedence over preemptive and proactive security measures.

The struggle against violent Islamic fundamentalists will take place abroad, but as the events of the last decade make clear, attacks will also take place at home. Open communication with immigrant communities is critical for investigation and prevention of terrorism. A surveillance society is likely to alienate these communities. It is crucial to remember that there are two objectives: to save the lives of our citizens and not to lose independence and stability as a nation.[134] This war against violent religious fundamentalists will not be won without the cooperation of domestic immigrant communities.[135] The vast majority of members of these communities are law-abiding U.S. citizens, but as Heymann observes, "[i]n terms of national well-being, the gravest national dangers from a terrorist act (short of an immense escalation of terrorist tactics), are that the interplay of terrorism, public reaction, and governmental response may sharply separate one significant group from the rest of society."[136] In such situations, Heymann notes, "the terrorists will find it far easier to secure communication channels, [etc.]."[137]

As Gilles Kepel observed, "[t]he most important battle in the war for Muslim minds during the next decade will be fought not in Palestine or Iraq but in these communities [of second-generation Muslims] on the outskirts of London, Paris, and other European cities."[138] So far, the United States has been spared home-grown terrorism from violent Islamic fundamentalists; Britain has not. It is instructive to briefly

133. These include the White House. NATIONAL INFORMATION SYSTEMS PROTECTION PLAN, VERSION 1.0 (January 7, 2000); REPORT OF THE PRESIDENT OF THE UNITED STATES ON THE STATUS OF FEDERAL CRITICAL INFRASTRUCTURE PROTECTION ACTIVITIES (January 2001); NATIONAL STRATEGY TO SECURE CYBERSPACE (September 17, 2002).

134. Heymann, *supra* note 130, at xi.

135. *Id.* at 101-02.

136. *Id.* at 2.

137. *Id.* at 13.

138. GILLES KEPEL, THE WAR FOR MUSLIM MINDS 8 (2004).

consider the difference between the Muslim communities in the two nations.

In Britain, South Asian immigrants are three times as likely to be unemployed as white Britons; indeed, forty percent of Pakistani women in Britain are unemployed, as are twenty-eight percent of Pakistani men.[139] But in the United States, the incomes of people of Pakistani origin are close to the median in New York and slightly exceed the median in New Jersey.[140] Britain was a non-immigrant society until after the Second World War. In the United States, by contrast, the South Asian population is following in the footsteps of the many immigrant groups that preceded them, moving up the socio-economic ladder generation by generation. In Britain, the South Asian population is isolated from British society; in the U.S., it is far more integrated. Kepel observes that "it is imperative to work towards full democratic participation for young people of Muslim background."[141]

However, that democratic participation is threatened by domestic intelligence-gathering practices. The warrantless foreign-intelligence wiretaps conducted by the NSA raised fears in the Arab-American and Muslim-American communities. Mountzer Sleiman, a journalist at Al Mustaqbal Alarabi ("The Arab Future"), noted that bin Laden had not been able to recruit Arab or Muslim Americans, but said that, "[the community] feel[s] they are being profiled, under threat, under constant harassment." Sleiman wanted to know if it was "open season on the Arab American and Muslim American in the United States."[142] Such fears in the Arab-American and Muslim-American communities should worry law enforcement. Terrorists seek to split society and then use the split toward their own ends.

The United States is a diverse, multicultural society, woven from many strands. What has held this complex society together is respect for the rights of others, notwithstanding such events as the lynching and state-government-authorized violence against black citizens in the South and the shameful internment of Japanese-Americans during the Second World War. Although early U.S. government responses to the September 11th attacks did not characterize the attacks as a Muslim problem, later government actions have forged a different perception. According to Professor Peter Skerry of Boston College, "events since 9/11 — special registration programs, the Patriot Act, and the war in

139. Nina Bernstein, *In American Mill Towns, No Mirror Image of the Muslims in Leeds*, N.Y. TIMES, July 21, 2005, at A1.

140. *Id.*

141. KEPEL, *supra* note 138, at 295.

142. Questions and comments following remarks by General Michael Hayden, former NSA director, at the National Press Club, Washington, D.C. (Jan. 23, 2006).

Iraq — almost require even secular families in this second generation [of South Asian immigrants] to construct an American identity as Muslims."[143] This is potentially dangerous and without doubt complicates terrorist investigations.

Investigating terrorism cases often means conducting an investigation where the first serious criminal activity – doctored passports and lapsed visas do not count – is often the *only* criminal activity. How do investigators find these people? One way is, of course, the age-old method of following connections. The connections between Khallad Sheik Mohammed, a senior bin Laden security official, and "someone named Midhdar" brought Nawaf al Hazmi and Khalid al Midhdar, two of the September 11th hijackers, to the CIA's attention prior to the September 11th attacks. But another avenue is connections with the community. To be successful, investigators must rely on the good will of the people. As experience in Israel and Northern Ireland shows, harsh investigative techniques – massive searches and surveillance, abuses of prisoners under detention, ill-treatment in jail – often backfire.[144] In Northern Ireland, for example, many believe that the advantages gained through this policing were "offset by the effect of stimulating IRA recruitment."[145]

Sleeper cells pose a particularly serious threat to Western societies, and their investigation requires painstaking work in a community largely composed of law abiding citizens. The need for community cooperation increases many times over when the problem is sleeper cells. Surveillance techniques reminiscent of the repressive regimes that many in the Muslim community fled when they came to the U.S. are likely to alienate the very people who can most aid domestic law enforcement investigations.[146] Building eavesdropping capabilities into the Internet, which undermines such fundamental American values as privacy and freedom of association,[147] will not engender trust in Muslim communities.

In conducting a war against violent Islamic fundamentalists, we must consider what aspects of this war can be won, and what can only be won at too high a cost. Security solutions that also have high adverse social impacts may return much less than they cost in terms of societal cohesiveness and community cooperation. Applying CALEA to VoIP is one such instance.

143. Bernstein, *supra* note 139.

144. HEYMANN, *supra* note 130, at 132, 141-42.

145. *Id.* at 126.

146. Europe, particularly Germany and France, have significantly larger Muslim communities than does the United States. In order for these nations to successfully investigate violent fundamentalists, police will need the cooperation of the local communities.

147. *See, e.g.*, NAACP v. Alabama, 357 U.S. 449 (1958).

Thinking clearly about which acts can be prevented and which cannot is crucial. Timothy McVeigh's attack on the federal office building in Oklahoma City was the work of a very small group of people. The al Qaeda attacks of September 11th, on the other hand, involved the coordination of a much larger group. Unless we move to a surveillance society on the scale of the former East Germany, a move that runs counter to most of what we hold dear about this country, we will never be able to fully protect against attacks by a "lone" warrior like McVeigh We need to factor such common sense into our thinking about security.[148] Thus, while one can expect surveillance tools to help prevent activities on the scale of September 11th, this is less true for activities carried out by a small group. Depending on the size of the group involved in the London transport bombings, for example, such acts might not be discernable without a level of surveillance intolerable in a free society.

Laws authorizing law enforcement wiretapping were originally passed because of the threat of organized crime.[149] Organized crime works through a small cadre of tightly-linked workers, often family members. This makes the organization difficult to penetrate and complicates investigations. Since radical Islamic fundamentalist groups appear to pose similar investigative difficulties, wiretapping is a particularly tempting tool. But there are also serious differences between investigating organized crime and violent religious fundamentalists, differences that change the value of wiretapping in investigations.

Law enforcement has a far greater deterrent effect on domestic organized crime groups than on those espousing violence as a way to achieve a fundamentalist society. Organized crime does not seek to destroy modern society; terrorists do. A severe disruption of Western democracies would be a major victory for the violent Islamic fundamentalists. And, as discussed earlier, imprisonment is not the same deterrent for violent Islamic fundamentalists for as it is for organized crime figures.

The fact is that wiretapping is unlikely to provide much benefit in tracking terrorists. Al Qaeda is well aware of the eavesdropping and targeting capabilities of the U.S. military and has learned the dangers of communicating electronically. Bin Laden, for example, does not use the

148. HEYMANN, *supra* note 130, at xxi-xxiii.

149. Title III was passed in response to the President's Commission on Law Enforcement and the Administration of Justice, and the original set of crimes that could be investigated using wiretaps were serious crimes that were part of the repertoire of organized crime, e.g., racketeering or interstate transport of stolen goods. The Senate Judiciary Committee Report on Title III said that "each offense was chosen because it was intrinsically serious or because it is characteristic of the operations of organized crime," HOUSE REPORT 90-1097 at 97 (1968).

telephone but instead relies on hand-written messages delivered by trusted couriers. Many terrorist communications are already sufficiently brief and difficult to decipher, not because of digital encryption, but because the communications are written in a code known to the insiders but not to the surveillers.[150]

Thus, in fact, content may not be necessary. Investigators have been quite successful in tracking terrorists without being able to hear the contents of their messages. In a 2002 case, investigators tracked al Qaeda members through terrorists' use of prepaid Swisscom phone cards. These had been purchased in bulk, anonymously. But when investigators discovered through a wiretap on an intercepted call that "lasted less than a minute and involved not a single word of conversation" that they were on to an al Qaeda group, the agents tracked the users of the bulk purchase.[151] The result was the arrest of a number of operatives and the breakup of al Qaeda cells.

This example illustrates what the national security community realized years ago. In the age of electronic communications, wiretapping is a rich and fruitful investigative tool when you can get it, but the critical need to secure civilian infrastructure has the side effect that the contents of wiretapped communications will become increasingly inaccessible to investigators.[152] Instead, traffic analysis – who is communicating with whom – will become the more valuable tool. Traffic analysis can reveal an organization's structure, its membership, even the roles of its members, and can do so in a way that benefits the investigators without such negative impacts on the civilian infrastructure.

The actions of al Qaeda are ". . .on a scale approaching war, but they were committed by a loose, far-flung, nebulous conspiracy with no territories or citizens or assets that could readily be threatened, overwhelmed, or destroyed."[153] This war will likely see other destructive actions on the scale of September 11th or substantially worse. In the face of such a war, the United States needs to think carefully about the impact of the choices it makes. Many times, when the nation was threatened,

150. A case in point is the September 11th hijackers. Mohamed Atta described a nuclear facility as "electrical engineering" to his fellow pilots (NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *supra* note 126, at 245). Khalid Sheikh Mohammed used the code of send "the skirts" to "Sally" to instruct another al Qaeda member to send funds to Zacarias Moussaoui. The targets were discussed as if the participants were students at a university: the Pentagon was "arts," the World Trade Center, "architecture," the Capitol, "law," and the White House, "politics." *Id.*, at 246, 248.

151. Don Van Natta, Jr, & Desmond Butler, *How Tiny Swiss Cellphone Chips Helped Track Global Terror Web*, N.Y. TIMES, March 4, 2004, at A1.

152. This realization is undoubtedly part of the reason for NSA acquiescence to the change in cryptographic export-control regulations in 2000.

153. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *supra* note 126, at 348.

the response was to diminish citizens' freedoms. But, as the Church committee pointed out in the mid 1970s, "[p]ersons most intimidated by well not be those at the extremes of the political spectrum, but rather those nearer the middle. Yet voices of moderation are vital to balance public debate and avoid polarization of society."[154]

In the face of nihilistic threats from violent religious extremists, it is imperative to encourage voices from the middle. Moving to a surveillance society runs a serious risk of irreparably harming democratic participation. The security of the United States will face unprecedented challenges if ubiquitous surveillance has the effect of shutting down the voices of moderation from the immigrant communities. We cannot afford to take such a risk.

If you only have a hammer, everything looks like a nail. The FBI is primarily a crime-fighting agency rather than a crime-prevention one. Thus, the FBI has pressed for the extension of CALEA to VoIP. But this is the wrong tool at the wrong time, and its usage will create dangers rather than alleviate them.

CONCLUSION

In considering wiretapping and other surveillance technologies, it is crucial to remember that the United States has two objectives: to save the lives of its citizens and not to lose independence and stability as a nation.[155] The application of CALEA to VoIP is not only an abrupt change in U.S. wiretap law, but also represents an anomaly in U.S. communications law.

From the very early days of the republic, the United States has treated communications as something of the people, for the people, and by the people. The Postal Act of 1792 established two fundamental principles: privacy of the mails – postal officials were not allowed to open mail unless the mail was undeliverable – and low rates for newspapers, thereby encouraging the dissemination of political information to the hinterlands. Thus the United States departed sharply from the governments of Britain and France, neither of which provided any such safeguards. Indeed, in Europe the postal service was a system of government surveillance. By contrast, the U.S. Post Office was seen as a facilitator of democracy and was one of the few strong federal institutions established in the nascent United States.[156]

The differences between European and U.S. communications systems extended to the development of new technologies. While in

154. INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, *supra* note 25, at 291.

155. HEYMANN, *supra* note 130, at xi.

156. PAUL STARR, THE CREATION OF THE MEDIA 3 (2004).

Europe, the telegraph system was a mechanism of state security,[157] that did not occur in the United States. In Europe, the telegraph system was government owned;[158] in the U.S., privately. In Europe, the adoption of new communications systems was slower and less geographically extensive; the major cities were connected, but not so the small towns and rural areas.[159] In America , small towns and rural areas enjoyed all the benefits of new communications systems.

The fact that the United States spanned a continent is a partial explanation for the rapid development of new communication systems; it was simpler to achieve integration in one nation than in many with competing regulatory systems. Other factors were at work as well, including the deeply held conviction that the spread of knowledge would aid in success the nation's democratic values. But a bedrock reason for the growth of telecommunications in the United States is the privacy afforded to communications. This spawned trust in the use of these communication systems, and a growing dependence on them.[160]

Nonetheless, the government can still read citizens' mail. Spying on the mails was a sufficient problem that in 1825 Congress felt obliged to address it. The Church Committee uncovered numerous instances of law enforcement and intelligence agencies reading private mail without a search warrant,[161] but the law has always been on the side of privacy. The 1825 Postal Act[162] made prying into another person's mail illegal. In 1878,[163] the Supreme Court ruled that the government could not open first-class mail without a search warrant. The FBI's efforts on CALEA undermine a 220 year tradition in this country of safeguarding privacy in communication systems.

The negative effects of applying CALEA to VoIP will ripple though the public and private sectors of America. It poses risks to the economy through the potential loss of corporate information. U.S. national security is threatened through the potential enabling of cost-effective massive intelligence gathering. There is a risk to the freedom of U.S. citizens. This echoes the risks Europeans faced because of the Echelon network. Echelon is an eavesdropping network run by the U.S., U.K., Australia, Canada, and New Zealand, that targets civilian

157. In order to conduct surveillance, European governments typically banned the use of ciphers. *See id.* at 159.

158. In Britain, the telegraph was initially private, but in 1870, Gladstone's government bought the private lines. *Id.* at 168.

159. *Id.* at 227.

160. *Id.* at 228.

161. A Resolution to Establish a Committee to Study Government Operations with Respect to Intelligence, S. Res. 21, 94th Cong. 62, 107 (1975).

162. Act of March 3, 1825, 4 Stat. 102.

163. Ex Parte Jackson, 96 U.S. 727 (1878).

communications;[164] its existence became public in the late 1990s. When that occurred, European governments sought to secure their private-sector communications and they liberalized their cryptographic export-control policy (so that the E.U. nations would be able to purchase security equipment from one another). The private sectors' need for communications security outweighed national-security and law-enforcement needs to conduct domestic wiretaps. The United States liberalized its cryptographic export-control policies shortly afterwards.

To law enforcement, it may seem obvious that wiretap laws should automatically be updated with each change in communications technology. Looking at the issues more broadly, this is far from clear. Wiretap laws were passed at particular times to satisfy particular sets of problems. As technology and society change, so must our laws. Society's security needs are not enhanced by requiring that VoIP implementations be CALEA-compliant. Rather, the CALEA requirements applied to the Internet are likely to cause serious harm to security, industrial innovation, and the political efforts in the war against violent Islamic fundamentalists. Among the first principles of security should be: "First, do no harm." The proposed CALEA requirements do not pass this test, and should not be approved.

164. Duncan Campbell, *Interception 2000: Development of Surveillance Technology and Risk of Abuse of Economic Information*, Report to the Director General for Research of the European Parliament, Luxembourg (April 1999), *available at* http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm.