THE LARGE IMMORTAL MACHINE AND THE TICKING TIME BOMB

SUSAN LANDAU[*,†]

* I am extremely grateful for the many discussions I have had with John Treichler, which greatly helped hone the ideas in this paper. I am also very appreciative for insights and suggestions made to me by David Clark, Al Gidari, Mike Jacobs, and Brian Snow. Their thoughts, and the background information they and John shared, were invaluable. I would also like to thank Matt Blaze, Scott O. Bradner, and Micah Sherr for suggesting various improvements and suggestions. I presented this paper as the fifth annual Privacy Lecture at UC Berkeley, School of Law, sponsored by the Berkeley Center for Law and Technology (BCLT). I am quite grateful for the opportunity, and want to thank the participants at the BCLT annual privacy lecture for their suggestions. I particularly want to thank Paul Schwartz for his suggestions.

† Author's current affiliation: 2012 Guggenheim Scholar. This work was done, in part, when I was an Elizabeth S. and Richard M. Cashin Fellow at the Radcliffe Institute for Advanced Study at Harvard University, and when I was a Visiting Scholar in Computer Science at Harvard University.

INTRODUCTION

In 1994 Congress passed the Communications Assistance for Law Enforcement Act (CALEA).[1] In many ways a rather extraordinary law, CALEA provides "a telecommunications carrier shall ensure that its equipment, facilities, or services . . . are capable of – (1) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept . . . all wire and electronic communications carried by the carrier within a service area."[2] In other words, the law puts the government in charge of determining interception standards for telephone switches. Compliance with the accepted standards provides carriers with a safe harbor.[3]

One particularly odd aspect of the law is its approach to time. Under CALEA, switches in use were to be retrofitted to accommodate the new requirement.[4] In this the government took into account the fact that telephone switches last. But although the longevity of switches was acknowledged in the funding aspect of the law, longevity of switches was considered only retrospectively.

The Cold War had ended, and the discussion during the legislative process focused on law enforcement's concern that they would need to maintain the ability to wiretap despite changing communications technology. The possibility that security threats would develop against the telecommunications infrastructure itself does not appear to have been discussed during CALEA's passage. That building surveillance capabilities into civilian communications networks constituted a major

1. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1010).

2. 47 U.S.C. § 1002(a) (2008). The law goes on to say in § 1006, "[a] telecommunications carrier shall be found to be in compliance with the assistance capability requirements under section 1002 of this title, and a manufacturer of telecommunications transmission or switching equipment or a provider of telecommunications support services shall be found to be in compliance with section 1005 of this title, if the carrier, manufacturer, or support service provider is in compliance with publicly available technical requirements or standards adopted by an industry association or standard-setting organization, or by the Commission under subsection (b) of this section, to meet the requirements of section 1002 of this title." *Id.* § 1006(a)(2).

3. *Id.* § 1006(a).

4. The law includes reimbursement to the carriers for doing so. *Id.* §§ 1003(e), 1007(c)(3)(A). This reimbursement was crucial in the telecommunications carriers dropping their opposition to the bill; an earlier bill, the Digital Telephony Act of 1992 had failed to receive a single congressional backer, in part because of carrier opposition (there was also opposition from civil-liberties organizations). Roger van Bakel, *How Good People Helped Make a Bad Law*, WIRED, Feb. 1996, at 135, *available at* http://www.wired.com/wired/archive/4.02/digitel.html.

security risk was essentially ignored. That lapse has proved increasingly problematic.

As is now well known, creating access to communications switches can lead to unauthorized eavesdropping.[5] Intruders using interception capabilities built into a Vodafone Greece cell phone switch eavesdropped upon the cell phones of over one hundred senior officials of the Greek government including the prime minister and the head of the ministries of the interior and defense for a period of ten months in 2004-2005.[6] In 2010 Tom Cross, an IBM researcher, found errors in a Cisco wiretapping architecture for IP networks,[7] a system that was already in use by service providers around the world. The system was designed for law-enforcement interception and was based on standards designed by the European Telecommunications Standards Institute (ETSI).

The vulnerabilities described above are well known. Much less well known is that U.S. communications switches are also at risk. It is required that communications switches used by the US Department of Defense be submitted to the National Security Agency (NSA) for testing before they can be deployed. When several large switch manufacturers submitted CALEA-compliant switches to the NSA for testing – a requirement prior to use in Department of Defense systems – the NSA found security problems with the CALEA-compliant implementation on *every* single switch submitted for testing.[8]

In some sense, the lack of attention to changing threat models is not a surprise; the notion that the communications infrastructure might be the subject of an active attack is relatively new in the commercial world. During the development of the Internet, for example, eavesdropping was considered the main security risk. Thus, provision of confidentiality, integrity, and authentication services dominated early thinking about Internet security, and there was no attempt to design against attacks on the system itself.

In another sense, the lack of attention to the potential of attacks on the switches is surprising. Since 1988, when a graduate student at Cornell University released a worm (a self-replicating program) that

5. Some of this material appeared in Susan Landau, *Legally Authorized Wiretapping—but Not Communications Insecurity*, *in* PATRIOTS DEBATES: CONTEMPORARY ISSUES IN NATIONAL SECURITY 143, 146 (Stewart Baker et al. eds., 2012).

6. The capability was built into switches purchased from the Swedish telecommunications company Ericsson. Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair*, IEEE SPECTRUM, July 2007, at 26, 27.

7. Tom Cross, *Exploiting Lawful Intercept to Wiretap the Internet*, BLACK HAT (2010), http://blackhat.com/presentations/bh-dc-10/Cross_Tom/BlackHat-DC-2010-Cross-Attacking-LawfulI-Intercept-wp.pdf.

8. Private communication with Richard George, Former Technical Director for Information Assurance, National Security Agency (Dec. 1, 2011) (on file with author).

brought down ten percent of the then existing Internet,[9] we have increasing evidence not only that Internet security threats exist, but that they take a form considerably more complex than eavesdropping. Attacks include those that "take over" user machines and attacks on Internet infrastructure that disrupt availability of resources. Modeling the potential security threats is now becoming standard practice when developing new information technology products and services.[10]

CALEA, however, is part of the Public Switched Telephone Network (PSTN) world. For decades, the security focus of telecommunication service providers was on reliability and protecting against theft of service. By the 1990s, changes in communications technology, including the rise of the Internet, and changes in the communications business, including the rise of small communications providers, were already fundamentally altering the business of securing telecommunications. But the Internet culture of threat modeling does not appear to have made it over to the telecommunications world either during the crafting of CALEA or in the development of the standards that accompanied its implementation.

Because electronic switches are expensive and last a long time,[11] the situation is actually somewhat worse. The policies of the regulatory system unintentionally impede fast responses to new security threats.[12] Public utility commissions handle the cost of new infrastructure by amortizing rates based on the technology's expected lifetime. This is effective so long as one can reliably predict the infrastructure lifetime (and the infrastructure functions with normal upkeep). But the fact that threat modeling was not taken into account in the cost structure of the switches presents an additional impedance to securing CALEA-compliant switches.

The seriousness of the security lapse has become apparent with hindsight. During the last decade, cyberexploitation, an intelligence-gathering activity that can include the theft of intellectual property including business plans, research, and patent data, has become an increasing threat to the United States. That threat stayed largely in the background until the middle of the last decade. In 2005 *Time* magazine

9. John Markoff, *Living With the Computer Whiz Kids*, N.Y. TIMES, Nov. 8, 1988, http://www nytimes.com/1988/11/08/us/living-with-the-computer-whiz-kids html?sec=technology&spon=&pagewanted=1.

10. *See, e.g.*, Adam Shostack, *Experiences Threat Modeling at Microsoft*, (Sept. 28, 2008), *available at* http://download microsoft.com/download/9/D/3/9D389274-F770-4737-9F1A-8EA2720EE92A/Shostack-ModSec08-Experiences-Threat-Modeling-At-Microsoft.pdf.

11. For example, consider the fifth-generation switch, 5ESS, was first sold in 1985 and whose sale was only discontinued recently. Private communication with John Treichler, Chief Technical Officer, Applied Signal Technology (Jan.9, 2011) (on file with author).

12. SUSAN LANDAU, SURVEILLANCE OR SECURITY?: THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES 188-89 (2011).

reported that in October 2004 someone scanned various U.S. military computers to determine which machines were vulnerable because they had particular unpatched software, and that on November 1, at 10:23 pm (PST), the vulnerabilities were exploited by outsiders, who in a series of four cyberexploitations over six-and-a-half hours, probed computer systems at U.S. Army Information Systems Engineering Command at Fort Huachuca, Arizona, the Defense Information Systems Agency in Arlington, Virginia, the Naval Ocean Systems Center in San Diego, California, and the United States Army Space and Strategic Defense installation in Huntsville, Alabama, stealing various types of sensitive and classified information.[13] *Time* reported there had been a series of network break-ins at U.S. military sites and defenses contractors including Lockheed Martin, Sandia National Labs, Redstone Arsenal,[14] and NASA.[15] The stolen files took circuitous routes, but all seemed to end up in southern China.[16]

This story was the first public description of what has become a major onslaught.[17] In January 2010 Google announced an intrusion and the theft of some of its proprietary code. In fact similar intrusions and cyberexploitations had already been conducted against a wide swath of U.S. businesses and government sites, including Adobe, BP, Conoco Philips, Disney, Dow Chemical, DuPont, ExxonMobil, General Dynamics, General Electric, Intel, Johnson & Johnson, Juniper Networks, Morgan Stanley, Northrup Grumman, Oak Ridge National Laboratories, RSA, Sony, Symantec, and Yahoo.[18]

---

13. Nathan Thornburgh, *Inside the Chinese Hack Attack*, TIME, Aug. 25, 2005, http://www.time.com/time/nation/article/0,8599,1098371,00 html.

14. This is home to Army Aviation and Missile Command.

15. Nathan Thornburgh, *The Invasion of the Chinese Cyberspies*, TIME, 34, Sep. 5, 2005, *available at* http://www.time.com/time/magazine/article/0,9171,1098961-1,00 html.

16. *Id.*

17. BRYAN KREKEL, NORTHROP GRUMMAN, CAPABILITY OF THE PEOPLE'S REPUBLIC OF CHINA TO CONDUCT CYBER WARFARE AND COMPUTER NETWORK EXPLOITATION (2009), *available at* www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

18. Ariana Eunjung Cha & Ellen Nakashima, *Google attack part of vast campaign; Targets are of strategic importance to China, where scheme is thought to originate*, WASH. POST, Jan. 14, 2010, at A01 *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html (listing Adobe, Dow Chemical, Northrup Grumman, Symantec and Yahoo as targets of attack); Fahmida Y. Rashid, *HBGary E-mail Says DuPont Hit by China's Operation Aurora Attack*, EWEEK.COM (Mar. 11, 2011), http://www.eweek.com/c/a/Security/HBGary-Emails-Say-DuPont-Hit-by-Chinas-Operation-Aurora-Attack-306724/ (revealing information that Disney, DuPont, General Electric, Intel, Johnson & Johnson, Juniper Networks, Morgan Stanley and Sony were affected); Kim Zetter, *Top Federal Lab Hacked in Spear-Phishing Attack*, WIRED (Apr. 20, 2011, 1:16 AM), http://www.wired.com/threatlevel/2011/04/oak-ridge-lab-hack (detailing that Oak Ridge National Laboratory was a target); Michael Joseph Gross, *Enter the Cyber-dragon*, VANITY FAIR (Sept. 2011), http://www.vanityfair.com/culture/features/2011/09/chinese-hacking-201109 (stating that BP, Conoco Phillips, Exxon Mobil, General Dynamics and RSA were also

In August 2010, the Department of Defense signaled its concern with these issues. Writing in *Foreign Affairs*, U.S. Deputy Secretary of Defense William J. Lynn III stated, "[a]lthough the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term."[19] The 2011 report on economic espionage by the Office of the National Counterintelligence Executive describes an "onslaught of computer network intrusions originating from Internet Protocol (IP) addresses in China"[20] and singles out China and Russia as being "the most aggressive collectors of US economic information and technology."[21] Russia was seen as a "distant second to China."[22]

Compromising a communications switch creates a problem of enormous scale. If intruders break into Lockheed Martin, they can copy and remove files from Lockheed Martin, files that may contain information vital to national security. If intruders can compromise a network switch at Lockheed Martin's communications provider, then the intruders will be able to eavesdrop on all unencrypted communications traveling through the switch: Lockheed Martin's *and* everyone else's.[23] This is the risk faced when a communications switch is penetrated.

Despite these problems, security of the surveillance mechanisms do not form part of the CALEA standard, a standard with which service providers must comply. Yet the risks are myriad.

When a single company fails to secure itself, it puts its intellectual property at risk. When a service provider has a security breach in its infrastructure, it puts *all* communications using the infrastructure at risk. PSTN switches that are CALEA compliant run the risk that private information will be exposed. This private information can simplify the type of targeted attacks used against U.S. industry and government facilities. Depending on configuration, CALEA compliance for facilities-based broadband or interconnected Voice over Internet Protocol (VoIP) communications may put other IP-based communications transiting the

---

attacked).

19. William J. Lynn III, Defending a New Domain: The Pentagon's Cyberstrategy, 89 FOREIGN AFF. 97, 100 (2010).

20. OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE 5 (2011), *available at* http://www ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf. (updating 14 ANN. REP. TO CONG. ON FOREIGN ECON. COLLECTION AND INDUS. ESPIONAGE (2008).

21. *Id.* at 4.

22. *Id.* at B-2.

23. *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 31-32 (2011) (statement of Susan Landau, Ph.D., Radcliffe Institute for Advanced Study, Harvard University).

switch at risk.[24] Given NSA's experience in testing CALEA-compliant switches, the threats described by Department of Defense Deputy Secretary Lynn means that CALEA compliance creates serious risks to U.S. national security.

Such a serious security lapse came about in part because the shifting nature of the threats against communications systems at the time of CALEA's passage. Part of that shift occurred due to the major transformations in espionage that have occurred in recent decades. During the Cold War, targets were originally military and government sites, but by the 1970s, Soviet interest grew to include the military contractors.[25] By the 1980s, other nations, including U.S. allies, had joined in on spying on U.S. companies; the purpose was often economic rather than military.[26]

That requirements placed on installed infrastructure shift over time is not new. What is distinctive in the CALEA case is the cause for the change. When bridges, municipal water systems, the power grid face changing requirements, the change is typically one of increased demand: heavier traffic, more water, shifting requirements as electricity usage increases. There may also be requirements for greater robustness as a result of a better understanding of the extremes that occur during earthquakes, hurricanes, floods, etc. The shift in security requirements for communications switches arises from the radically changing nature of the threats against the switching infrastructure.

We are now in a problematic security situation of our own making, one in which a law – CALEA – mandates a security vulnerability in U.S. communications infrastructure.[27] This is a serious national security risk, one that developed as a result of surveillance requirements that did not take into account the security risks such surveillance creates. This paper proposes technical and policy solutions to rectify the situation. That surveillance capabilities must themselves be secured lest they themselves

24. The CALEA functionality creates risk by adding complexity—always the bane of security—and because the wiretapping functionality afforded by CALEA may itself be subverted. This is discussed in detail in section III(A).

25. THOMAS R. JOHNSON, AMERICAN CRYPTOLOGY DURING THE COLD WAR, 1945-1989: BOOK III: RETRENCHMENT AND REFORM, 1972-1980, at 145 (1998) *available at* http://www nsa.gov/public_info/_files/cryptologic_histories/cold_war_iii.pdf.

26. Pierre Marion, the former director of the French intelligence agency, Direction Generale de la Securite Exterieure explained that, "[i]t would not be normal that for us to spy on the United States in political matters or in military matters, but in the economic and technical spheres, we are competitors; we are not allies." INTERAGENCY OPSEC SUPPORT STAFF, *Economic Espionage*, *in* IOSS INTELLIGENCE THREAT HANDBOOK 30, 37 (2004), *available at* http://www fas.org/irp/threat/handbook/economic.pdf.

27. The FBI has expressed interest in extending CALEA's scope to include not only switches but also communications applications. *See, e.g.*, Charlie Savage, *U.S. Tries to Make it Easier to Wiretap On the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1 *available at* http://www nytimes.com/2010/09/27/us/27wiretap html?pagewanted=all.

put society at risk is a lesson broader than securing CALEA-compliant switches. In a surveillance-prone world, it is a lesson we ignore at our peril.

The world of telecommunications is very technical, and, in order to clarify the security risks that CALEA compliance creates, I begin in section 2 by discussing the engineering history of the telephone switch; I go into some detail to explain some of the security mechanisms that were developed – and that have been undone so that switches might achieve CALEA compliance. In section 3, I sketch the convoluted history of CALEA's passage and implementation in order to show how security threats were ignored in the law's development and implementation. One surprising aspect of this that requires surveillance be built into communications infrastructure is that the nation's premier electronic-surveillance agency, the NSA, was not involved in CALEA's framing, a situation I describe in this section. In section 4, I discuss the security problems arising from building surveillance capabilities into a communication switch, while in section 5 I provide recommendations for improving the security of CALEA-compliant telecommunications switches. In addition, I also address the more general concern of securing critical infrastructure in light of changing threat models.

I. THE LARGE IMMORTAL MACHINE

Originally phone switching was done manually. A switch consisted of a panel of jacks that corresponded to phone "numbers" and cables that were used to connect the jacks; these connections were instituted by a human operator after a caller would request a connection. To make a call, the caller would pick up her phone and tell the operator with whom she wished to speak. The operator would ring the other party. If there was an answer, the operator would create a connection by patching a cable connecting the corresponding phone jacks. If the subscriber wanted to speak with a person at a different telephone office, then the operator needed to call through to an operator at that office. The operator at the other office would ring the other party. If the party answered, the operators would connect a trunk line between the two phones offices, and then patch the call through the jacks at each switchboard.

Such systems do not scale. Yet the telephone company's move to automation was slow.[28] Mechanical switching was not even developed by the Bell System, but instead introduced by a Kansas City undertaker,

28. According to the Bell System's official history, "the first half century of the telephone was dominated by manual switching systems and equipment." A.E. JOEL, JR. ET AL., BELL TELEPHONE LABS., A HISTORY OF ENGINEERING AND SCIENCE IN THE BELL SYSTEM: SWITCHING TECHNOLOGY (1925-1975) at 7 (G. E. Schindler, Jr. ed. 1982).

who was concerned that business was going to a rival.[29] Adoption of the automated switch took time. The Bell System did not have a fully automatic phone exchange until 1922, and four years later – the fiftieth anniversary of the telephone – only twenty percent of the telephone system used dial systems.[30]

Instead, the Bell System's emphasis was on reliability. So while various automatic electromechanical switching systems were being developed around the world, the Western Electric Company, the telephone company equipment supplier, focused on developing electromechanical switching systems that would aid operators in the central office.[31] In 1913, Western Electric filed a patent on "coordinate" switching equipment,[32] a set of contacts arranged in a matrix. The first commercial use of such a switch occurred in 1935 as "concentrator and call distributor" for trunk lines.[33] Bell Lab engineers optimized the switching fabric. This new crossbar switch became the switch of choice. This happened in the United States in the 1950s and in the rest of the world shortly afterwards. Then the computer era arrived.

A. The Conversion to Electronic Switching

In 1945 AT&T's Bell Laboratories began developing an electronic telephone switch to replace the electromechanical ones then in use.[34] AT&T had a number of requirements for the new switch. It had to be functionally equivalent to the switch in use while being economically competitive with these systems for a "significant segment of the market."[35] Since immediately replacing all of the old systems at the same was out of the question, the new switch needed to be backwards compatible with the electromechanical switches.[36] The new switch also had to meet the same reliability standards the electromechanical switches had satisfied.[37]

Meeting these criteria was complicated. AT&T prided itself on reliability standards that tolerated no more than two hours downtime in forty years.[38] Because of the differences between electromechanical

29. Brenda Maddox, *Women and the Switchboard*, *in* THE SOCIAL IMPACT OF THE TELEPHONE 262, 272 (Ithiel de Sola Pool ed., 1977).

30. *Id.*

31. JOEL, *supra* note 28.

32. *Id.* at 59.

33. *Id.* at 65.

34. W. Keister et al., *No. 1 ESS: System Organization and Objectives* 43, 45 BELL SYS. TECHNICAL JOURNAL 1831, 1832 (1964).

35. *Id.*

36. *Id.* at 1833.

37. *Id.*

38. W.O. Fleckenstein, *Foreword* to A.E. JOEL, JR., BELL TELEPHONE LABORATORIES, A HISTORY OF ENGINEERING AND SCIENCE IN THE BELL SYSTEM, SWITCHING TECHNOLOGY

components and computerized ones, this proved to be the most difficult aspect. Although capacity is reduced, if a part of an electromechanical switch fails, the switch itself still functions; a large percentage of communications can still be completed. By contrast, an electronic telephone switch is a processor running a stored program. Failure of the computerized processor would mean total failure of switching capability,[39] which was an unacceptable outcome.

AT&T's solution was to duplicate all units within the switch necessary for the switch's proper functioning.[40] Operational checks ensured that the equipment was functioning properly. If a malfunction was detected, special fault-recovery programs quickly determined the errant piece of equipment, switching it out of service, and turning on the duplicate.[41]

This solution took two decades to develop. In 1965 AT&T introduced No. 1 Electronic Switching System (ESS), a digital switch capable of routing one hundred thousand calls an hour.[42] Programmability of the switches has meant much greater flexibility and ease in adding new capabilities.[43] Including programmability in a switch increases security risks significantly; an issue I will return to later. Each new generation of switches was "backwards compatible," supporting the features of previous generations of switches.[44] Conversion to electronic switching was major news and even merited a front-page story in the *New York Times.*[45]

B. Signaling Systems 6 and 7

By the end of 1967, No. 1 ESS was operating in nineteen offices, eighteen in the U.S. and one in Montreal.[46] It was well on its way to being standard in every telephone company *central office* (the local phone exchange). Meanwhile, a new challenge had emerged.

In the 1960s, AT&T became the victim of "blue box" attacks in

(1925-1975), at xi (G. E. Schindler, Jr. ed. 1982).

39. Keister et al., *supra* note 34, at 1833.

40. *Id.*

41. JOEL, *supra* note 28, at 251.

42. This number was determined through surveying operating telephone companies and observing that fifty percent of the telephone lines were found in centers with nineteen thousand lines or more. Economies of scale meant that two 50,000-line units were only slightly more expensive than one 100,000-line unit, and so it was not particularly useful to have the switches grow too big. An upper size limit of 65,000 lines was placed on the switch. Keister et al., *supra* note 34, at 1834.

43. JOEL, *supra* note 28, at 412-13.

44. *Id.*

45. Robert Alden, *A Shift to All-Electronic Phones Begun in Biggest Step Since Dial*, N.Y. TIMES, Sept. 20, 1964, at A11.

46. JOEL, *supra* note 28, at 269.

which a caller could fool the phone company's signaling mechanism into allowing toll-free calls. This was accomplished through imitating the phone company's signaling tone, either by whistling down the line at the right frequency[47] or through a "blue box," an electronic device that simulated the signal of 2600 Hz. on the main trunk line to signal availability to other lines in the network and used other tones to signal the numbers the fraudster actually wished to dial.[48]

To obtain a free toll call, a caller would dial an 800 (toll free) number. This would trigger the process of charging for the call (note that it was the owner of the 800 number who pays for such a call). Before the call was actually completed, the fraudster would send another 2600 Hz. signal down the line. This would signal the trunk line (the line connecting switching offices) that the caller was disconnecting and would disrupt the connection. The trunk line would stop the dialing process. At this point, the caller would halt the 2600 Hz. signal. The trunk would wait for new dialed digits. This time, however, the fraudster would dial the digits of the number they wished to call. These were no longer limited to the 800 number; they could be anywhere in the automatic dialing system. However, because the accounting system remained engaged, this meant a new call would not be charged to the caller. Instead, at the end of the call, the accounting system charged the owner of the 800 number for the call – even though the call to the toll-free number had never been completed.[49] The underlying reason that such an attack could succeed was the control signals for the call – the 2600 Hz. signals on the line – were carried "in-band" through the same communications channel as the customer's voice.

One way to solve this problem was to separate call set-up information from the voice communication. Such a solution is in fact, a very natural way to architect a network. Separating content from control can enable faster call set up, and better network management and control.[50] It also enables the provisioning[51] of a wide range of network services, such as charging calls to credit cards, 800 numbers, etc. Finally, such a solution is better for security. By enabling control mechanisms

47. A toy whistle in Captain Crunch cereal boxes also signaled at 2600 Hz. and could be used.

48. In addition to the blue-box attacks, there was a simpler "black-box" system used by Nevada bookmakers that used only the 2600 Hz signal.

49. Ron Rosenbaum, *Secrets of the Little Blue Box*, ESQUIRE, Oct. 1971, at 119-20.

50. On the other hand, in-band signaling affords the flexibility of being able to introduce new services without changing the control plane (this is what has enabled the ability to easily introduce new Internet applications).

51. In the telecom world, "provisioning" means the initial set up of resources to enable providing services to a customer. Thus the establishment of SS6/SS7 common channel signaling provisions the network to enable the various services of charging to credit cards, 800 numbers, etc.

and content to travel in separate paths, attacks, including unauthorized wiretapping, become more complex.[52]

Signaling System 6 (SS6), has two channels: one for call content such as voice, the Call Content Channel (CCC), and one for call set-up information, the Call Data Channel (CDC). After SS6's adoption in 1975, the blue-box problem disappeared.[53] SS6 has since been replaced by Signaling System 7 (SS7), a versatile standard more adaptable for digital communications that continues the use of the two-channel architecture of SS6.

C. Separating Control Data from Content

Engineering works best when things are kept simple.[54] Separating call control data – including the number to be called and the number doing the calling – from call content is an instantiation of this principle. AT&T first implemented this separation using a crossbar switch in 1935; this was extended to toll calls in 1943.[55] The concept, a scaled version of SS6 named "Common Channel Interoffice Signaling," was introduced to the full network in the 1970s.[56]

Envision Common Channel Interoffice Signaling has two parallel planes; for simplicity, imagine one above the other. The bottom plane is the "*control plane"* handling call management, while the top plane is the "*data plane,"* managing call content (in other words, the conversation). When a call comes into the control plane, it sends a signal to the next appropriate switch to establish a connection. If the subscriber being called responds, the connection is established. Except for the fact that the connections are now happening electronically, this part of the system is quite similar to what occurred using the telephone systems of the 1890s. But here is where the distinction arises.

Instead of call content traveling over the same channel as the signaling information, the content travels on the data plane. For this to occur, when the connection has been established, the control plane signals the data plane to set up the communications connections. Communication then happens over the data plane. Until the call ends, the control plane remains uninvolved in the communication. When the call is completed, the data plane signals the control plane. The control plane then signals to dismantle the circuit.

---

52. Indeed, the control channels could even be encrypted.

53. Or perhaps manifested itself in the Internet hacking that developed a short time later.

54. HENRY PETROSKI, SUCCESS THROUGH FAILURE: THE PARADOX OF DESIGN 4-5 (2006).

55. The first commercial application of the crossbar switch occurred in New York City. JOEL, *supr*a note 28 at 65. The extension to toll system occurred in Philadelphia. JOEL, *supr*a note 28, at 83.

56. JOEL, *supra* note 28, at 321.

The control plane communicates not only with the data plane about starting and ending the call; it communicates with central billing to transmit information (and perhaps also to find out information); it checks the switch's status and health. The latter can include the temperature of the circuit cards, the number of calls completed per unit time, etc. The processors on the control may have physical interfaces to other cards in the system where these measurements are made, but these limited connections (limited in the sense of minimal data transfer of a very fixed type) are not considered to violate the model of separating the control and data planes.

This clean architecture is an example of good engineering. While it might at times appear more efficient to combine functionalities into a single system, the best way to ensure a system works properly is to separate different functionalities into different components. As Henry Petroski, the dean of engineering failures, has written, "[m]ost things have more than a single purpose, which obviously complicates how they must be designed and how they therefore can fail. The more complicated the design problem, naturally the more difficult the solution and hence the more likely that some details and features may be overlooked, only to have their absence come to the fore after the thing is manufactured or built and put to the test of use."[57]

The other important aspect of good engineering design is to minimize the number of communications between the components. Such design simplifies debugging the system when things go wrong (as they inevitably do).

It is worth repeating that the separation of content and control also minimizes the ability of others — e.g., eavesdroppers — to intrude upon the system as long as others do not gain control of the control system. A further benefit is that as long as system interfaces are minimized, different parts of the system can be updated as needed, swapped in or out, etc.[58] Note, though, that this is true in any system with clean interfaces between components.

D. Maintaining the Immortal Machine

For over a century, the phone company was a completely vertically integrated company. In 1880 the American Bell Telephone Company purchased Western Union's telephone-manufacturing subsidiary,

57. PETROSKI, *supra* note 54, at 4.

58. This same principle underlies the network-layering model of the Internet. The fact that everything runs on IP (Internet Protocol) and IP runs on everything is a large part of the reason that innovation has flourished on the Internet. Steve Hotz, Rodney Van Meter & Gregory Finn, *Internet Protocols for Network-Attached Peripherals*, 3 (1998), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.10.7527.pdf.

Western Electric Company of Chicago, and, in 1882, the two companies agreed on a system in which no one else could play. [59] The telephone company agreed to buy its phones from Western Electric, while the manufacturer agreed to limit its sales to American Bell and its franchises.[60] From the point of view of the telephone company, such monopolistic practices simplified the business. With divesture came an increase in the number of switch manufacturers.[61] AT&T/Western Electric, Nortel, Siemens, Alcatel, and Ericsson entered the fray. This created complexity.

Another complexity was longevity of telephone switches. While cell phones, laptops, desktops, and even servers are replaced every few years, central office switches remain in service for decades. Designers of the initial electronic communications switches nicknamed the switches "large immortal machines" because of their longevity.[62] The first digital toll switch, the 4ESS, was introduced in 1976[63] and the last 4ESS was installed in 1999,[64] while the first fully digital central office switch, the 5ESS, was introduced in 1982 and was sold until at least 2000.[65] Many 5ESS and some 4ESS are in use to this day.

Typically a service provider will purchase a service contract for switch maintenance along with the purchase of a telephone switch. The usual annual cost is about 10% of the cost of the switch. This cost is factored into the rate settings determined by the state public utility commissions.

Switches evolve. One of the attractions of building a switch in software is the ease of modifying it for new functionality.[66] Developing new services costs money, but putting new functionalities into a switch can be charged to the customer. So public utility commissions do not need to concern themselves with switch updates for new services at the time they set prices based on a new switch. Updating for security is a different story, however.

Nothing technical precludes updating a switch if a vulnerability is discovered. But providing a patch to a switch already in place does not generate additional revenue (though it does cost money to provide the patch). So although there is urgency – an unpatched vulnerability creates a risk and is one service providers cannot delay in fixing – the lack of

59. Martin Fransman, *Evolution of the Telecommunications Industry*, *in* 3 WORLD TELECOMMNS. MKTS.: INT'L. HANDBOOK OF TELECOMMNS. ECONS., 16 (2003).

60. *Id.*

61. This was a proximate cause for CALEA.

62. W. Keister et. al., *supra* note 34, at 1841.

63. A.J. Spencer, Jr., *Prologue*, 56 BELL SYS. TECH. J. 1015 (1977).

64. *History of Network Switching*, AT&T, http://www.corp.att.com/history/nethistory/switching.html (last viewed December 16, 2011).

65. Treichler, *supra* note 11.

66. This malleability is also what makes a switch so easy to subvert.

recompense means that the system is incentivized against discovering and fixing problems in any software, including the wiretapping software.

To understand the CALEA conundrum – how a law to improve security was introduced without developing a mechanism to counter the communications insecurities it creates – we must understand the law's genesis. A brief history of CALEA is in order.

II. CALEA'S CONTROVERSIAL PASSAGE

The 1968 Omnibus Crime Control and Safe Streets Act, Title III of which establishes warrant procedures for wiretaps in criminal investigations, does not address whether telecommunications providers had to cooperate with law enforcement upon the provision of a wiretap warrant.[67] That matter was settled by Congress, who in 1970 added a provision that "[a]n order authorizing the interception of a wire, oral, or electronic communication under this chapter shall . . . direct that a provider of wire or electronic communication service . . . shall furnish the. . .technical assistance necessary to accomplish the interception False."[68] This did not, however, answer the question of whether communication systems equipment and design had to include the ability to perform legally authorized eavesdropping.

For many years, the technical ability to wiretap had not been seriously in question. Telephone communications emanated from the local central office. This provided a clear place from which to install a wiretap. If they were technical problems installing a wiretap, they were "addressed on a case-by-case basis in negotiations between the local monopoly service provider and law enforcement."[69]

The 1984 divesture of AT&T and rise of the regional Bell operating companies (RBOCs) introduced a period of rapid innovation in telecommunications services and a sharp increase in the number of providers. In 1992 the FBI asserted that law-enforcement agents were facing increasing technical difficulties in executing authorized wiretaps. A 1994 investigation by the Government Accounting Office (GAO) concurred that there were technical problems in "tapping a variety of services or technologies, including call forwarding, fiber, and ISDN" and insufficient capacity for wiretapping cellular calls.[70]

The FBI presented a list of 183 instances in which it encountered difficulties in performing authorized wiretaps, including 54 cases where there was insufficient capacity at a cellular switch, 4 cases in which a

67. 18 U.S.C. § 2510-2512 (2012).

68. District of Columbia Court Reform and Criminal Procedure Act of 1970, Pub. L. No. 91-358, § 211, 84 Stat. 473, 654 (codified as amended at 18 U.S.C. § 2518 (2012)).

69. H.R. REP. NO. 103-827, at 14 (1994), *reprinted in* 1994 U.S.C.C.A.C. 3489, 3495.

70. *Id.*

cellular provider could not intercept a long-distance call made to a cellular phone, 33 cases where dialed digits could not be captured simultaneously with audio, 20 cases in which speed dialing, voice dialing, and call waiting presented problems.[71] I take a brief technical detour to explain how wiretapping is performed.

A. How to Wiretap

When the PSTN was run by electromechanical switches, wiretapping required a physical intrusion. There are actually many choices as to where to wiretap. If there was access to the communications device (e.g., the phone or computer), then the simplest place to put a tap is within the communications device itself.[72] Using bugs hides the fact that wiretapping is occurring, and works as long as the battery-operated bug has power. Otherwise one has to wiretap.

One can wiretap by placing alligator clips to connect into the phone lines at the phone junction box or anywhere along the path to the central office. The problem with that option is that, unlike the bug placed in the phone, wiretapping paraphernalia is visible. In particular, telephone company personnel may discover the tap and disable it.

Traditionally the next place to tap is the main distributing frame (MDF), which is where, in modern telephony, subscriber phone lines coming into the central office are placed in numerical order. A wiretap consisted of a *loop extender*, a tap creating a logical fork on the subscriber's line, with one feeding directly to a monitoring location. This method of wiretapping was no longer effective once more modern telephony services that operate at the switch, such as call forwarding,[73] were employed. The technical difficulties encountered by law-enforcement agents in exercising legally authorized wiretaps motivated CALEA.

B. The CALEA Proposal

The U.S. signals intelligence agency, the National Security Agency (NSA), has many roles. It is primarily known for its codebreaking capabilities, but an equally important aspect of NSA is its role in information assurance, securing national-security communications and systems.

It was this role that brought the NSA into advising U.S. law enforcement on the potential consequences of the shift to digital

71. *Id.* at 16-17.

72. This was what was done in the original intrusion into the Democratic Party headquarters at the Watergate.

73. Because the call does not proceed down the local loop to the subscriber, a wiretap at the MDF will not have access to the communication.

telephony.[74] Beginning in 1990 Clinton Brooks, assistant to the Director of NSA, briefed FBI officials on the shift to digital communications technology and the impact this could have on wiretapping.

One issue was encryption. For decades the U.S. government had indirectly controlled the domestic use of encryption through controls limiting what computer and communications products could be exported; by limiting what could be exported, the government effectively prevented strong cryptosystems products from being deployed for domestic use.[75] The dispute over this issue began in the 1970s, but came to a head in the 1990s. Industry and academia had been battling NSA over the issue, but the FBI now also began to press publicly for controls on the domestic use of encryption.

But being able to decrypt communications was useful only if one could first obtain the communications. By 1992 the FBI had grown very concerned over its ability to wiretap digital telephone networks. The FBI proposed a "Digital Telephony" bill that required wiretapping capabilities be built into digital telephone switches. The draft bill required that all telecommunications providers[76] design their system to accommodate wiretaps, and that the system enable remote delivery of the intercepted communications. Costs were to be borne by the carriers.

This was a surprising proposal in many ways. Previous wiretapping law concerned delimiting the set of circumstances under which the government could eavesdrop. This bill was about mandating technological requirements. More surprisingly, there apparently had been no consideration of the security risks that might be created as a result of building wiretapping capabilities into a telephone switch. The NSA had not been consulted on the technical aspects of the bill prior to its introduction.[77] This was remarkable. Although the more well-known role of the NSA is signals intelligence – extracting intelligence from opponents' communications – an equally important role in providing national security is played by the Information Assurance Directorate (IAD) of the NSA, the side of the agency that protects U.S. national-security communications and systems. Yet the IAD was not consulted during the drafting of CALEA.

With opposition from service providers and civil-liberties

74. Private conversation with Clinton Brooks, Senior Technical Advisor, National Security Agency, January 17, 1997; further details may be found in WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 83-84 (updated and expanded ed. 2007).

75. *See* Whitfield Diffie & Susan Landau, *The Export of Cryptography in the 20th and 21st Centuries*, *in* THE HISTORY OF INFORMATION SECURITY: A COMPREHENSIVE HANDBOOK 725, 725-36 (Karl de Leeuw & Jan Bergstra eds. 2007).

76. There was an exemption for private branch exchanges.

77. Private communication with Clinton Brooks, Former Senior Technical Advisor, National Security Agency, November 10, 2011.

organizations, the bureau was unable to acquire any Congressional sponsors for its Digital Telephony proposal. Two years later the FBI returned with a bill. This time the NSA policy office was advised of the bill, but NSA was not asked to provide a technical analysis of the proposed legislation.[78]

The new bill, which included authorization for $500 million to aid service providers in converting their switches to meet new surveillance standards, disarmed one set of opponents. Opposition by the service providers melted away. On the last day of the 103rd session, the Communications Assistance for Law Enforcement Act passed.

C. Controversy over Implementing CALEA

CALEA's implementation proved difficult. Privacy advocates, service providers, and law enforcement were in prolonged dispute over which surveillance capabilities were to be standardized. Disagreements arose over many features including whether location information was to supplied for cellular calls[79] and whether *post-cut-through digits* (digits dialed after initial call set-up) were to be included in data transmitted to law enforcement, etc.

Privacy advocates and service providers thought the issue of location information had been determined before the law's passage: section 103(a)(2) of CALEA states that information acquired for a pen register or trap-and-trace order "shall 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)." But law enforcement argued for a more expansive standard that included origin, direction, destination, and termination of the communication.[80]

On the issue of post-cut-through digits, the conflict was over content versus signaling information. Clearly sometimes post-cut-through digits were content — e.g., a bank account number, a prescription renewal number, a passcode to access voicemail — and in those cases, a pen register should not suffice for obtaining the data. Law enforcement countered with the observation that many times such dialed digits were, in fact, signaling information, e.g., the number dialed after reaching one's service provider of choice. This was particularly common

78. Private communication between Clinton Brooks, Former Senior Technical Advisor, National Security Agency, November 30, 2011.

79. The J-standard included the ability to report location at the start and completion of a call, but not any other location information, including a change of cell towers during the call.

80. This is the standard definition used by law enforcement for the term "call-identifying information." *See,* e.g., AUDIT DIV., OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, THE IMPLEMENTATION OF THE COMMUNICATION ASSISTANCE FOR LAW ENFORCEMENT ACT 1, Audit Report No. 06-13 (2006), *available at* http://www.justice.gov/oig/reports/FBI/a0613/final.pdf.

in the 1990s when the number of providers of long distance proliferated.

Working with law enforcement, a subcommittee of the Telecommunications Industry Association (TIA) spent over two years developing Joint Standard 025, Lawfully Authorized Electronic Surveillance(J-standard).[81] Given the controversy over what should be included in the standard, it was no surprise that the result did not please the disputing parties.

Privacy and civil-liberties advocates filed a petition with the Federal Communications Commission (FCC) over insufficient privacy protections in the J-standard.[82] Telecommunications service providers asked for clarity on the rule making as well as an extension on implementation dates.[83] And the Department of Justice filed a petition with the FCC over insufficient surveillance capabilities (law enforcement sought to include additional capabilities into the standard, including post-cut-through digits).[84]

In August 1999, the FCC issued its CALEA order acceding to most of what law enforcement sought.[85] Telecommunications providers filed suit, but lost.[86] However, the court's ruling chastised the FCC for insufficiently explaining the rationale for the items included in the CALEA requirements and ordered the commission to provide explanation for the requirements.[87] It did so. The TIA responded by making the 1998 list of FCC requirements an amended TIA standard, JSTD-025A. Although this set of standards was now the law, deployment continued to be slow.

D. Security Requirements for CALEA

CALEA includes a high-level security provision. The law requires that telecommunications carriers "ensure that any interception of communications or access to call-identifying information effected within its switching premises can be activated only in accordance with a court order or other lawful authorization and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with regulations prescribed by the Commission."[88]

---

81. Albert Gidari, *Designing the Right Wiretap Solution: Setting Standards Under CALEA*, 4 IEEE SECURITY AND PRIVACY 29, 31 (May/June, 2006).

82. Communications Assistance for Law Enforcement Act, *Public Notice*, F.C.C. Docket. No. 97-213, DA-98-762, 2-3 (April 20, 1998).

83. *Id.* at 3.

84. *Id.* at 3-4.

85. Communications Assistance for Law Enforcement Act, F.C.C. Docket No. 97-213, 14 FCC RCD.16, 794 (2001).

86. U.S. Telecom. Ass'n v. F.C.C., 227 F.3d 450, 465 (D.C. Cir. 2000).

87. *Id.* at 465-66.

88. Communications Assistance for Law Enforcement Act, 47 U.S.C.A. § 1004 (1998).

The security provision was not followed up prescriptively. Because development of the J-standards were marked by attention to cost and vendor neutrality, the FCC sought to minimize the technical requirements that CALEA-compliant implementations would be required to satisfy. Thus, the standards for interception were written to accommodate a span of architectures (and vendors). As a result the specifications were less precise with respect to security requirements than they might have been.[89] In places the specifications were shockingly lacking. Because there was no presumption that a telecommunications provider would have a mechanism for key exchange between law enforcement and the provider, the J-standard stated, "[t]here is no requirement to provide message integrity to ensure that the message has not been altered in transmission," and "[t]here is no requirement to provide message sender authentication to ensure the integrity of message sender identification."[90]

All engineering system designs include Interface Control Documents (ICDs) that delineate the inputs and outputs between different components of the system. ICDs are well known for being porous, that is, they not only let through the communications that should be allowed, but often many others as well. In the case of CALEA-compliant switches and data routers, such porousness is quite dangerous, for this can lead the way to permitting unauthorized access to communications (either transactional information or content).

In designing – and building – a CALEA-compliant switch, ICDs should be carefully and completely locked down to limit communications to the ones necessary, permitting no others. Then the systems need to be rigorously tested against allowing unintended access. Because this involves anticipating unanticipated circumstances, such design and testing is difficult to do. And there is also a tendency to avoid expending effort on the design and testing because security does not directly contribute to the bottom line.

Threat modeling against the CALEA-compliant switches was not required. Threat modeling is the methodology of determining and assessing security risks that may impact the system. It requires a systematic understanding of the attributes of the system, of the attackers,

89. Telecomm. Indus. Ass'n, TR45 LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE ANSI J-STD 025A (2003), at 34-35. (In the section on information flows within the network, the J-standard states, "[t]he Access Function typically includes the ability . . . to protect (e.g., prevent unauthorized access, manipulation, and disclosure) intercept controls, intercepted call content and call-identifying information consistent with TSP [telecommunication service provider] security policies and practices" and similarly "[t]he Delivery Function typically includes the ability to protect (e.g., prevent unauthorized access, manipulation, and disclosure) intercept controls, intercepted call content and call-identify information consistent with TSP security policies and practices.").

90. *Id*. at 16.

their capabilities, and their goals and techniques.[91] In a changing environment such as presented by a telephone switch with updates, threat modeling cannot happen once, but must occur each time a change occurs in the system. This is complicated by the fact that the change may not occur in the providers' system, but in systems with which the switch interacts. Thus, fairly frequent tests and "red teaming" (penetration testers used to check a system's security) would appear to be a natural part of CALEA security requirements. But no such requirements are part of the J-standard.

CALEA occurred against the backdrop of the "Crypto Wars" – the battle waged between the government and industry and academia over the public's ability to use strong forms of encryption to protect their communications[92] and the expansion of the Internet from a research project funded by the Defense Advanced Projects Research Administration to the commercial entity it is today. This change was accompanied by a shift of power — as sometimes happens when a new technology emerges — from established companies (the telecommunications providers) — to the innovators involved in developing the new technology. In this case, the Internet Engineering Task Force (IETF) included many of these innovators.

The IETF develops Internet standards that enable communications to seamlessly travel across the network of networks that is the Internet. The IETF began in 1981 as a group of government-funded researchers. Its current membership includes many from industry, academia, and elsewhere. In 2000, in light of CALEA and other efforts to develop wiretapping standards, the IETF examined whether wiretapping requirements should be included in the design of IETF standards. IETF standards are, as the name might suggest, based on engineering practice. The IETF concluded that building surveillance capabilities into a communications protocol did not make sense from a technical standpoint,

"The IETF believes that adding a requirement for wiretapping will make affected protocol designs considerably more complex. Experience has shown that complexity almost inevitably jeopardizes the security of communications; there are also obvious risks raised by having to protect the access to the wiretap. This is in conflict with the goal of freedom from security loopholes."[93]

As Al Gidari, privacy partner at the law firm of Perkins Coie LLP,

91. KAREN MERCEDES GOETZEL, ET AL., DEF. TECHNICAL INFO. CTR SOFTWARE SECURITY ASSURANCE: A STATE-OF-THE-ART REPORT 130 (2007).

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

93. INTERNET ENGINEERING TASK FORCE, RFC 2804, IETF POLICY ON WIRETAPPING 2 (May 2000).

has so aptly put it, "[t]he notion of engineering a back door into a communications system for anything other than troubleshooting or maintenance [is] the equivalent of designing a security flaw into the product."[94]

It is worth noting that wiretapping is not the only code that might enable intrusions; code for system maintenance and troubleshooting might also inadvertently introduce security flaws. These functionalities are, however, necessary for communications system support.

E. The Next Stage: Voice over IP

After the JSTD-025A battles, the next set of CALEA disputes involved VoIP – the use of packet technology to transmit voice over the Internet. That this situation arose was perhaps unexpected. During the 1994 CALEA hearings, FBI Director Louis Freeh had been explicit about what law enforcement was not seeking, "communications between private computers, PC-PC communications not utilizing a telecommunications common net, would be one vast area, the Internet system many of the private systems that are evolving. Those we are not going to be on by the design of this legislation."[95] Senate Judiciary Committee member Larry Pressler asked, "[a]re you seeking to be able to access those communications also in other legislation? Freeh responded, "[n]o, we are not. We are satisfied with this bill."[96]

Thus, CALEA limits applicability to telecommunications providers. The law has an exemption for "information services," defined as:

> (A) meaning the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications; and
>
> (B) includes —
>
> (i) a service that permits a customer to retrieve stored information from, or file information for storage in, information storage facilities;
>
> (ii) electronic publishing; and
>
> (iii) electronic messaging services; but
>
> (C) does not include any capability for a telecommunications carrier's internal management, control, or operation of its telecommunication network.[97]

---

94. Gidari, *supra* note 81, at 30.

95. *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Strategies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before The Subcomm. on Tech. and the Law, Comm. on the Judiciary and Subcomm. On Civil and Constitutional Rights of the House Comm. on the Judiciary* 103rd Cong. (1994), (testimony of Louis Freeh, Director of the Fed. Bureau of Investigation).

96. *Id.*

97. 47 U.S.C.A. § 1001(6)(A)-(C) (1998).

Section 103(b)(2) of CALEA states that "[t]he requirements of subsection (a) [capability requirements] do not apply to — (A) information services."

The FBI's commitment to limiting CALEA to telecommunications providers did not last. In a 2003 letter to the Federal Communications Commission, the bureau stated it was increasingly unable to wiretap VoIP communications.[98] Four months later the Department of Justice, FBI, and Drug Enforcement Administration petitioned the FCC to clarify the services and entities to which CALEA applied.[99] Arguing that CALEA had a broader definition of communications carrier than the Telecommunications Act of 1996,[100] DoJ, FBI, and DEA contended that "switching" was therefore broader than "circuit switched" and encompassed packet switching as well.[101] Law enforcement argued that this broader definition of telecommunications carrier should include broadband services providing access to the public Internet through high-bandwidth packet-switched systems.[102]

Surprisingly the FCC concurred. By relying on a clause in CALEA stating that a telecommunications carrier included entities providing replacement for a substantial portion of the local telephone exchange service,[103] the FCC concluded that Congress had indeed intended the scope of telecommunications carriers to be broader under CALEA than under the definition of the 1996 Telecommunications Act.[104] This distinction was important as the FCC was not in a position to regulate information services. With this reasoning, the commission concluded that "facilities-based" broadband carriers and managed VoIP providers fell under the substantial replacement clause[105] and that facilities-based broadband and interconnected VoIP, services that connected with the PSTN, were thus subject to CALEA.[106]

Others disagreed. Universities were concerned that the definition of "all broadband Internet service providers" would include them (and make them effectively telecommunications service providers under CALEA). The American Council on Education, civil-liberties groups,

98. Letter from Martin J. King, Office of the Gen. Counsel, Fed. Bureau of Investigation to Marlene Dortch, Secretary, F.C.C., Re: Notice of Ex Parte Presentation Wireline and Cable Modem Broadband Internet Access Proceedings F.C.C. Docket Nos. 02-33, 95-20, 98-10 & CS Docket 02-52, 10-11 (July 11, 2003).

99. Joint Petition for Rulemaking to Resolve Concerning the Communications Assistance for Law Enforcement Act, *In re* U.S. Department of Justice, Fed. Bureau of Investigation, and Drug Enforcement Administration, RM No. (Mar. 10, 2004).

100. Telecommunications Act of 1996, Pub. L. No.104-104, 110 Stat. 56 (1996).

101. *Id.* at 12.

102. *Id.* at 15.

103. 47 U.S.C.A.§ 1001(8)(B)(ii) (1998).

104. 20 F.C.C. Rcd. § 16,318 (August 5, 2005).

105. *Id.* at 3-8.

106. *Id.* at 44, 47-48.

and some of the computer and telecommunications community filed suit against the FCC ruling. They lost. In a two-to-one decision, the U.S. Court of Appeals ruled in favor of FCC.[107] Though the ruling meant that CALEA would be applied to facilities-based broadband interconnected VoIP, in fact the ruling was stronger than that; it meant that CALEA applied to any public networks providing a substantial replacement for the PSTN.[108] Although the FCC had chosen not to extend CALEA rules to pure peer-to-peer communications, it would appear that nothing in the Court of Appeals decision would have prevented the commission from having done so.[109]

By now there had been many CALEA battles. There had been fights over on Congressional intent, on privacy, on feasibility, and on costs, but no one had raised security considerations. This was a serious omission.

With the extension of CALEA to the Internet, the FCC greatly increased the security risks. It is to those issues I now turn.

III. WIRETAPPING IS AN ARCHITECTED SECURITY BREACH[110]

Three decades ago much of the U.S. telecommunications infrastructure was under the control of a single entity, AT&T, a regulated monopoly that did not face significant competition. During that period the company owned and operated the vast majority of the long-distance transmission lines and it operated two types of services over these: retail switched long-distance and long-term lease of "private lines" to private companies (e.g., the New York Stock Exchange) and governmental entities (e.g., the U.S. Department of Defense). The network was secured against a large variety of threats by three methods:

Physical security: The fact that AT&T long lines were carrying U.S. government data led to the requirement of securing and monitoring all AT&T switching and routing facilities.

Transmission security: Although the communications themselves were usually not encrypted, their transmission was typically resistant to

107. Am. Council on Educ. v. FCC, 451 F.3d 226, 235-36 (D.C. Cir. 2006).

108. *Id.* at 229.

109. The case turned on whether different forms of VoIP formed a substantial replacement for the PSTN and whether the FCC had the statutory authority to impose this extension of CALEA. *Id.* at 237-38. Peer-to-peer VoIP is not currently a substantial replacement for PSTN, and the FCC did not seek to extend CALEA to purely peer-to-peer communications. However, from purely a technical point of view, extending CALEA to peer-to-peer communications would be extremely difficult. *See e.g.*, Steven M. Bellovin, et al., *Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP*, 8 (2006), *available at* https://www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf.

110. Some of the material in the introductory part of this section appeared in different form in Steven Bellovin et al., *Can It Really Work? Problems with Extending EINSTEIN 3 to Critical Infrastructure*, 3 HARV. NAT'L SEC. J. 1 (2011).

interception.

Separation of content and control: SS6 and its successor SS7,[111] separated content and control. This makes wiretapping by an outsider more complicated, since the attacker has to control both the data and content channels. The separation also complicates an attacker's ability to manipulate the network.

The break-up of AT&T led to a situation in which the single phone company was replaced by a plethora of competitors. Currently there are four large service providers[112] – AT&T, Verizon, Sprint, and T-Mobile – and hundreds more ranging from medium (serving, say, a hundred thousand customers) to tiny (serving only hundreds to a few thousand customers). While during the period of the AT&T monopoly, there were also many medium and small providers; the situation is different now, for the complexity of securing the infrastructure has grown. Large providers are able to provide a modicum of security, but the small to medium size providers are much less in a position to do so. Since, as of late 2009, the United States had almost 1500 domestic ISPs with fewer than one hundred employees,[113] this presents an additional serious security problem.

Two other changes in communications have also changed the security equation (and this extends to the large providers as well). The first is that unlike in the 1960s and 1970s, data, rather than voice, is the prevalent transmission. The second is that transmission is now digital rather than analog. These two are not unrelated. One might expect that the fact that communications are digital would make it simpler to protect information.[114] But because of the fundamental design of the Internet, this turns out not to be the case. I will first explain how recent changes in telephony have made securing the network more difficult and then turn my attention to actual breaches.

A. CALEA Confuses Switch Functionality

Modern telephone switches are expected to perform switching functions, including advanced services such as call forwarding, call waiting, call hold, and call conferencing, highly reliably. CALEA-compliant switches are expected to accomplish these tasks while also deploying authorized third-party interception on any communications

111. SS7 has both international and nation-specific versions.

112. After divestiture, AT&T was broken up into seven regional Bell operating companies (RBOCs); there were also other phone companies, such as GTE. These recombined in a number of ways. In addition, the rapid growth of wireless communications led to new players, multiple mergers, and much churn in the telecommunications industry.

113. OneSource search conducted on January 6, 2010.

114. This is because early systems for voice communication encryption spent a high percentage of their work converting voice from an analogue signal to a digital one.

transiting the switch. The latter must be done so that it is invisible to the party being intercepted.[115]

This places a great deal of work on the control plane, which must support communications (with other switches) to establish and takedown call circuit, communications (with the data plane) to initiate and complete the call, communications with billing, communications with other circuit cards in the system to keep tabs on system health. For security and to ensure correctness, these functions should be strictly separated, e.g., separate memory, separate communication channels, etc.

CALEA specifications actually prevent such a clean security solution. Consider, for example, post-cut-through digits. From a purely technical standpoint, post-cut-through digits are content and thus should be transmitted on the data plane.[116] From the standpoint of CALEA, post-cut-through digits are treated as transactional data, to be supplied under a pen register and trap-and-trace order.[117] This breaks the clean architecture of two communications between the control plane and the data plane, one signaling the beginning of a call and the other signaling the call's completion. Call management software and call intercept software are intermingled, and the ability to clearly specify who should have access to data and the ability to carefully test (including security functionality) will be much more complex. This increases the risk that it will be done incorrectly or incompletely.

Recall that complexity is the bane of good security. Aside from directly interfering with the separation of functionality that a clean security design requires, CALEA also indirectly interferes with security through the added complexity it presents to switch functionality. If the communication system does not have good security to begin with, the addition of wiretapping capability to the switch makes that capability available to third parties.

Surprisingly it appears that the J-standard does not include requirements for auditable wiretaps. Neither is such material in

115. There are many ways that a target can discover its communications are being surveilled. The fictional HBO program "The Wire" illustrates one such way in the fictional case of Frank Sobotka, an official in the Baltimore longshoremen's union who is suspected of participating in illegal activity. He discovers that his cellphone account contains a note saying not to cut off service. This raises Sobotka's suspicions that he is being wiretapped, and he changes his behavior as a result. *The Wire: Duck and Cover* (Home Box Office broadcast July 20, 2003).

116. The astute reader might wonder how touch tones work in this environment; after all, touch tones are call signaling information that travel over the same wires to the telephone central office as the call content. That does not change the control plane/data plane model, however. At the telephone central office, the touch tones are processed and the resulting control signals are sent over the controller portion (the control plane) of the telephone switch. The model holds.

117. *In re* Communications Assistance for Law Enforcement Act, *Order on Remand*, 17 FCC Rcd. 6896, 6927 (2002).

associated product literature.[118] For security's sake, there should be a log file kept of all interceptions as well as access to the interceptions. Adding tamper-proof auditing capabilities does, of course, increase complexity of the system as well.

B. Vulnerabilities Resulting from Internet Architecture

All communications in the Internet, whether files, email, web pages, video, voice, or IM, are broken up into packets, small chunks of data that include the intended destination of the information. In theory (though less so in practice) each of these packets can travel a different path from source to destination. Packets include a sequence number and are reassembled at the destination to reform the complete piece of content.

Circuit-switched communications, the PSTN world, are superficially similar to the packet-switched Internet world of the Internet. They use the same type of transmissions facilities, the same type of routing and switching mechanisms to move communications.[119] However, the architectures of the two networks are very different. Telephone communications start by reserving a circuit through which the entire communication travels; that circuit is reserved for the duration of the communication regardless of whether it is being used at a particular moment. Packets do not. This lack of predictability of routing proves to be a major problem in mobile IP communications.[120] Even more problematic is the asymmetry of Internet routing: unlike telephony, the communication from Alice to Bob does not necessarily take the same path as the communication from Bob to Alice.

Other differences also complicate authorized wiretapping. The PSTN was built to guarantee voice quality, and so it minimizes the number of switches a call transits. The Internet was instead built to maximize information sharing. Then its developers emphasized reliability of data transmission and were much less concerned about the real-time aspect of the communication.

Internet designers focused much less than the PSTN engineers on maximizing the quality of the experience. In part, this was possible because of the Internet's flexibility. Designers of the Internet protocols did not need to know what type of application would be transmitted; only application developers did. Known as the end-to-end principle, this is the idea that the user application defines the quality needed for the

118. Adam Bates et al., *Accountable Wiretapping -or- I Know They Can Hear You Now*, INTERNET SOCIETY (February 7, 2012), http://www.internetsociety.org/sites/default/files/P09_2.pdf.

119. Bellovin et al., *supra* note 110, at 9.

120. *Id.* at 14.

application.[121] The Internet's underlying flexibility has enabled Internet innovation, supporting such diverse application as web pages, streaming video, VoIP, etc.

The Internet developers addressed reliability and availability. To the extent that Internet security was considered, interest lay in preventing communication eavesdropping.[122] Authenticating hosts, ensuring applications did not include malware, and protecting Internet infrastructure were simply not part of the agenda in developing the set of protocols enabling researchers to share resources (the original goal of the Internet).[123] It is an omission that has come back to haunt the Internet developers. One place where this is so is routers, the computers optimized for the job of sending packets across the network of networks.

The Internet is vast – billions and billions of devices. No router can possibly know the best routes for all destinations. So routers instead know local information: the routers to which it connects, and some information about where those are connected. From this routers make decisions on where to send packets. Routers store routing information in small databases – router tables – with the best routes to ranges of IP addresses; these tables are constantly updated as new devices are put on and removed from the network. As a result of its communication model, the Internet suffers from a number of insecurities, one of the more serious being the lack of authentication of routing information.

Another problem is the lack of authentication of endhost computers (also known as endhosts). This is a complicated issue. The strength and the source of weakness of the Internet is that it is not a centralized system like the PSTN. In the PSTN, where the phone calls are one-to-one communications, it makes sense to authenticate the end hosts — the phones — as to who they are; that is crucial for billing purposes.[124] In the Internet, which hosts a wide variety of communications — file transfers, emails, web browsing, VoIP, video streaming — there are many situations where it is counterproductive to authenticate first. One instance is commercial sites, whose main focus is traffic. Any action that

121. "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." J. H. Saltzer et al., *End-to-End Arguments in System Design*, 2 ACM TRANSACTIONS ON COMPUTER SYS. 277, 278 (1984).

122. LANDAU, *supra* note 12, at 39.

123. The Internet was a research project of the Defense Advanced Research Projects Administration (DARPA), a Department of Defense agency devoted to developing advanced technologies for the military. DARPA's intent was to build a network of different computers that could share resources with one another. There was no expectation at the time the project started in the 1960s that it would grow to encompass a world-wide network supplanting the PSTN.

124. For phones, this is done simply: by being connected to the end of an identified wire (for cell phones the situation is slightly more complicated).

requires the end user to authenticate themselves or their communications device before any transaction (including viewing the site) occurs is likely to significantly decrease traffic. Similarly authentication first makes even less sense for various government sites or libraries, where their role is to share information while *allowing the reader to be anonymous*. So the Internet, this network of networks, has to satisfy many differing needs, and the needs for authentication often differ. Sometimes this results in machines that should authenticate to each other not doing so. One result is that routers receive information from untrustworthy sources; far too frequently they do not have definitive routing information. As we shall see later, this increases the risks involved in wiretapping communications on IP networks.

The fundamental problem in secure Internet wiretapping, however, is that, unlike in the PSTN, communications data and content are intermingled in packet communications. On the routing processor itself there is an intermingling of control data and communications content. The clean architecture needed for security while wiretapping is impossible to achieve in Internet routers.

Until now my discussion of security risks engendered by building wiretapping capabilities into switches has been largely theoretical. But these risks are not just theoretical.

C. Real Breaches

The most serious appears to be the 2004-2005 wiretapping of one hundred senior members of the Greek government, including the Prime Minister. In purchasing a switch from Ericsson, Vodafone Greece had opted not to purchase the wiretapping capabilities. An update to the switch software included these capabilities, but, per contract, these were not turned on. Since the wiretapping was not to be enabled automatic auditing was not included.

The wiretapping was surreptitiously turned on. Whenever a call was made to or from one of the targeted numbers, the technology sent a duplicate to one of fourteen prepaid cellphones. The intruders installed a rootkit (a program with privileged access that stayed hidden) in the switch. They were thus able to update the wiretapping technology as needed.[125]

A different wiretapping scandal erupted at Telecom Italia, where six thousand people were illegally wiretapped between 1996 and 2006. Here the targets were politicians, businesspeople, financiers, bankers, journalists, and even judges.[126] Large dossiers were amassed on the

125. Prevelakis & Spinellis, *supra* note 6.

126. Piero Colaprico, *"Da Telecom dossier sui Ds" Mancini parla dei politici*, LA REPUBBLICA (January 26, 2007), http://www repubblica.it/2006/12/sezioni/cronaca/sismi-

targets. It appears that the purpose of this tremendous set of intrusions was blackmail by corrupt insiders. The numbers mean that one in ten thousand Italians was wiretapped. No major business arrangement or political deal was ever truly private.

The U.S. was not the only nation seeking to require interception interfaces in communications equipment; many nations in Europe had developed similar requirements, in part because of suggestions made by the FBI.[127] The European Telecommunications Standards Institute developed standards for interception, and Cisco, the U.S. company responsible for a high percentage of the routers in the Internet, developed a wiretapping architecture for IP-based networks that "provided a general solution that has a minimum set of common interfaces."[128]

In 2010 IBM researcher Tom Cross found a number of problems with the architecture.[129]

For example, a password was not necessary to obtain wiretapped information.[130] It was remarkably easy to do an insider attack since there was no audit trail and the output stream could go "anywhere."[131] Using relatively few tries, an outsider could determine a valid username and password. This would enable him to turn on the system and, bypassing the service provider's management network, have wiretapped information sent to his desired pick-up point.[132]

This problem came about because while the architecture recommended discarding wiretap requests that weren't of the correct format, this was not a requirement of the Cisco architecture and not all implementations followed the recommended implementation.[133] (This problem was discovered in 2008 but not all systems were patched.)[134] It

mancini-8/dossier-ds/dossier-ds html.

127. In 1993, prior to the passage of the CALEA, the FBI held a meeting in its research facility in Quantico on the issues surrounding interception of digitally switched networks. Representatives from the European Union nations, Canada, Sweden, Norway, Finland, Hong Kong, Australia, and New Zealand attended. *EU and FBI Launch global telecommunications surveillance system: "Launch Global Telecommunications Systems: 'Not a significant document" – UK Home Secretary*, 7 STATEWATCH BULLETIN, no. 1 (Jan.-Feb. 1997). Shortly over a year later, the European Union passed a resolution requiring realtime monitoring capabilities. The FBI fingerprints on this were unmistakable: the Memorandum of Understanding, which extended this agreement to any non-EU states interested in joining, pointed to the General Secretary of the EU Council and the FBI Director for any further information. *See* DIFFIE & LANDAU, *supra* note 75, at 225.

128. Fred Baker et al., *RFC 3924: Cisco Architecture for Lawful Intercept in IP Networks*, THE INTERNET SOCIETY (October 2004), http://www.rfc-editor.org/rfc/rfc3924.txt.

129. CROSS, *supra* note 7.

130. *Id.* at 16.

131. *Id.* at 25.

132. *Id.* at 15-19.

133. *Id.* at 19.

134. *Id.* at 20.

was easy to bypass audit systems for detecting unauthorized use.[135] What is striking about this particular set of problems is that Cisco had published the full set of specifications in 2004,[136] but the problems were not uncovered until several years later, after the architecture had already been deployed.

The insecurities arose as a result of several different issues. One was that, just as the CALEA requirements sought to accommodate a wide variety of switch designs, the Cisco interception standards sought to accommodate differing wiretapping requirements. The loosely defined architecture, which recommended —but did not require— encrypting interception requests, allowed an attacker to capture "any traffic on the [interception] device and route that traffic to any destination IP and port on the global Internet."[137] Another difficulty is that because of the flexibility inherent in the Internet's DNA, developing secure wiretapping standards for IP-based communications is even more difficult than developing similar standards for telecommunications. That has implications when the two systems, PSTN and the Internet, interconnect.

D. Additional Risks to Switches Due to Interconnection[138]

Such interconnection breaks the physical separation that had been used to provide security. For decades switches resided in protected telephone offices. Remote access was not an option. Beginning with the 4ESS the separation into control and data planes provided another form of security. But the convergence of the PSTN and the Internet is changing security.

The Internet has always relied on the underlying physical infrastructure of the PSTN. But for the first several decades of the Internet's existence, the switching and routing layers of the two networks were separate. Now, due to the 1996 Telecommunications Act and VoIP, this is changing.

The 1996 Telecommunications Act[139] requires that telephone companies permit connection to the SS7 infrastructure for a small fee. These fees are genuinely low. For example, in 2009 the cost to connect to the infrastructure in California was under $2000.[140] In 1996 no one

135. Private communication with Tom Cross, Researcher, IBM (Mar. 7, 2010).

136. In doing so, Cisco had eschewed security through obscurity. Although security through obscurity complicates attacks through hiding security mechanisms, it is not considered a good method for securing systems, since flaws are generally best found through public examination.

137. CROSS, *supra* note 7, at 4.

138. *See* LANDAU, *supra* note 12, at 128-130, 157, 180-181.

139. Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified in scattered sections of 15, 18, and 47 U.S.C.).

140. This included a $590 nonrecurring fee, $100 monthly charge, and a small mileage

considered that such an interconnection requirement would open critical infrastructure to attack. Consider the following two situations:

- In 1990 AT&T performed a software update of its 4ESS switches. A problem occurred. A switch signaled its neighbors it was out of commission, and then shortly thereafter signaled it was back. This confused the neighboring switches, which signaled their neighbors they were not working, which then went down, signaling their neighbors that they were not working, etc. Because the switches all had the same software—and thus had the same problem—the situation quickly cascaded, shutting down AT&T's long-distance service.[141]
- In 1997 a teenage hacker accessed a NYNEX switch in central Massachusetts— one that did not require authentication—and corrupted information in the switch. This disabled access to the Worcester Airport. The main radio transmitter was unable to communicate with the control tower, and incoming planes could not activate the runway lights. The airport was closed for six hours.[142] The problem arose primarily from a convergence of an old-style switching network—the PSTN—with new style control, and suffered from a lack of insufficient testing prior to deployment.

There are significant differences between what happened with the AT&T 4ESS and a potential attack on communications infrastructure. In the AT&T case, all switches were running the same software. They replicated the fault, creating a cascading situation. An attacker may not be in the position to compromise all switches in the system. But the low cost of entry to communications infrastructure required by the Telecommunications Act simplifies the ability of an attacker to compromise many switches, thus increasing his capability of creating a serious problem.

Because AT&T's software caused the problem, the phone company was in a position to easily fix that problem (which was to remove the problematic software until the bug could be fixed). If, however, an attacker implants the software in the switch, there is no easy way to determine which piece of software it might be. It may be in the system for years, lying dormant until activated.

VoIP presents a problem to E911, the U.S. emergency call system. The facilities that receive E911 calls, Public Safety Answering Points (PSAPs), are located around the nation. The PSAPs refer the call to the

---

charge.

141. PATRICK TRAYNOR ET AL., SECURITY FOR TELECOMMUNICATIONS NETWORKS 59-60 (2008).

142. Press Release, U.S. Dep't of Justice, Juvenile Computer Hacker Cuts Off FAA Tower at Regional Airport (March 18, 1998) (on file with author).

local first responders, which requires knowing the call location. Because call location is not explicitly included in the information in the call signaling data, a work-around was needed. This was easy. Phone location is kept by service providers for billing. A wire-line call transmits sufficient information to enable the PSAP to query a service location database and determine the caller's location.[143] This process is automated; when the PSAP operator answers the call, the caller's location appears on the operator's screen.

Since cell phones are mobile, the same technique does not work for them, and a different work-around is used. When a cellphone call connects to the PSTN, the call travels through a switch called the Message Switching Center (MSC). If the call is an E911 call, then the MSC assigns the cell phone a *pseudo number*, this number is from the same sector of the cell tower as the call is originating from.[144] The location of the pseudo number appears on the PSAP operator's screen, giving a current location for the mobile phone.[145]

VoIP is as mobile as cellphones are, so one might expect a similar solution for this Internet-based technology. But unlike cell providers, VoIP providers are competitors to telephone service providers, so it required an act of Congress to ensure that same access. Under the New and Emerging Technologies 911 Improvement Act of 2008[146] telephone companies are required to give VoIP providers the same interconnection access rights to E911 services that they offer to cellphone providers.[147]

The interconnection of VoIP to the E911 system does not in itself create a security risk (except perhaps for the ability to use E911 calls on VoIP to launch a denial-of-service attack on E911). But it is an example of the increasing interconnection of the Internet with the traditional PSTN, an interconnection that will only continue to grow. That means that the model of security— the phone company owning the switches with no one else accessing them and protecting them through physical security (no remote access permitted) — is no longer operative. But no system has been put in place in its stead. It is to that situation we now turn.

---

143. DALE HATFIELD, A REPORT ON TECHNICAL AND OPERATIONAL ISSUES IMPACTING THE PROVISION OF WIRELESS ENHANCED 911 SERVICES 4 (2002).

144. *Id.* at 19-20.

145. Using relative signal strengths at different cell towers provides a more accurate determination of location. More modern phones are equipped with GPS, which provides a still more accurate determination of location.

146. New and Emerging Technologies 911 Improvement Act of 2008, Pub. L. No. 110-283, 112 Stat. 2620 (2008).

147. Such a solution is not foolproof. For example, using a Virtual Private Network (VPN) to communicate will indicate the user is in the termination location of the VPN (say Google Headquarters in Mountain View) rather than where the user actually is (Beijing).

IV. CORRECTING THE SITUATION

Long-lived critical infrastructure is subject to risks unanticipated at the time of the technology's adoption. In the case of Internet-accessible infrastructure, risks are not only the natural ones of power outages and the like, but also directed attacks that seek to break, hack, and exploit systems. Former NSA Information Assurance Technical Director Brian Snow has remarked that"[t]here's malice out there trying to get you. When you build a refrigerator, you have to worry about random power surges. The problem is that Internet projects are designed assuming random failure rather than targeted attacks."[148]

PSTN switches are Internet-accessible refrigerators facing targeted attacks. Because an exploit against a CALEA-compliant switch may, as in the Greek wiretapping case, enable the interception of conversations transiting the switch, the value of a potential exploit is increased. The fact that a CALEA-compliant switch may allow remote access simplifies the process of exploitation. The fact that the capability for interception has been built into the switch increases the switch's complexity, making building the switch correctly substantially more difficult.[149] Potential problems abound.

For complex systems, security is always difficult to provide in the best of circumstances; security provided ex post facto is *never* sufficient. If security is not designed in from the beginning on a complex system, it is not difficult for nefarious developers, suppliers, or even your own people to install unexpected functionality. Such functionality may subvert the system.

In 2008 credit card readers were modified while being manufactured in China and Pakistan.[150] The readers were used for authenticating chip-and-pin credit cards used in Europe. These cards have an embedded microchip used to prevent card forgery. The customer types in a four-digit PIN code that is compared with the card's PIN that has been decoded by the card reader. A match means the card is legitimate.

Card readers used in Europe were modified to wirelessly transmit the card details to forgers, who cloned duplicate credit cards.[151] The tampered readers had been exported to Belgium, Britain, Denmark, Holland, and Ireland,[152] and the only visible difference between them and

148. Interview with Brian Snow, Former Information Assurance Technical Director, National Security Agency (Jan. 13, 2012).

149. INTERNET ENGINEERING TASK FORCE, *supra* note 93.

150. *See* LANDAU, *supra* note 12, at 172-73.

151. David Leppard, *Shoppers' Cards Hacked by Hi-Tech Pin Fraudsters*, SUNDAY TIMES, Oct. 12, 2008, at 4.

152. Henry Samuel, *Chip and Pin Scam 'Has Netted Millions from British Shoppers'*, TELEGRAPH (October 10, 2008), http://www.telegraph.co.uk/news/uknews/law-and-

the legitimate readers was a slight difference in weight—which meant investigators had to travel around Europe weighing card readers to weed out the tampered ones.

Modeling threats against telephone switches requires identifying potential attackers who are able to access the operating environment, and determining what their goals, potential techniques, and future attack patterns might be. It must include a deep understanding of all attributes of the switch software and hardware— and then collating that knowledge with the possible attackers. That a switch must be CALEA-compliant adds complexity to the threat-modeling process. Remote access and remote delivery aspects of the switch make it more difficult to defend, and the fact that the switch must be more complex further complicates securing it.

Although there were no requirements for threat modeling in the J-standard, undoubtedly some switch manufacturers did so out of due diligence. Their work was incomplete. As I have already noted, when several large switch manufacturers submitted CALEA-compliant switches to the NSA for testing, the NSA found vulnerabilities in the CALEA implementations of every single switch tested.[153] What this means is that it is highly likely that *every* switch not tested also had security problems; what it does *not* mean is that all the insecurities in the tested switches were found.

I turn to steps for improving the situation. I do so noting that the PSTN— and thus the switches inherent to circuit-switched communications— is coming to the end of its lifetime in the United States. The large immortal machines devoted to switching voice calls are being replaced by IP data routers (with servers doing the "control plane" function of converting the dialed phone number into the IP address of the destination). The issue of standards for secure communications interception remains. Indeed, as per section 4 of this paper, that may be even more important.

A. Developing Secure Communications Interception Standards

Certain principles follow for secure interception. Any interception system must be built with robust controls. There should be strict auditability built into interception systems. Finally, there should be strong controls on the remote delivery of content. I consider each of these in turn.

Robust controls first means a clean architecture in which the control network and data network are separated as much as possible. Within the

order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers html.

153. George, *supra* note 8.

control network, the design specification should maximize the separation between the control management software, which manages access to information, and all other applications.

ICDs should permit only the necessary communications between the control and data networks and no others. Because there is no physical separation between the transmission paths to control and data networks in data routers, it is especially important to keep communication separation between control management software and other applications.

Robust controls means that hardware tokens should be used for user authentication. Of course, there is a loss of flexibility created by not using software. However, in an interception system, robust controls trump flexibility. Hardware tokens would thwart the type of spoofing that Cross showed was possible in the Cisco architecture.[154]

Robust controls also means that two-party control should be employed for any multi-interception activities. That is, while a single user of the system may authorize a wiretap, two-party control should be used for user enrollment to the system.

Finally, robust controls mean that there should not only be two-party control for any multi-interception activities, but there should also be such control for any changes to the switch's control management software. Such controls might have prevented the 2004-2005 wiretapping breach at Vodafone Greece.

Strict auditability means there should never be group accounts. It should always be possible to trace activity to a named user, that is, an individual, who initiated interception activity.[155] This also means that policy should be in place that strongly backs up the non-sharing of user authentication credentials so that actions can always be traced to an individual user.

Strict auditability also requires that auditing mechanisms be automatically turned on whenever interception systems are activated or accessed. The auditing system should be tamperproof and the logs should be stored on a separate machine from the interceptions themselves. It should not be possible to turn off auditing capability, nor should it be possible to alter the auditing system's entries.

Strong controls on the remote delivery of content means that the transmission channel must be secured (strong cryptography, authentication) and that remote delivery cannot be initiated or intercepted without the robust controls described above.

These proposals may sound extreme. But consider DCS 3000, the FBI's system for wiretap data collection and management. Under Freedom of Information Act efforts undertaken by the Electronic

154. Cross, *supra* note 7, §II(D).

155. This means hardware tokens issued to a specific user, and not a role.

Frontier Foundation, certain internal FBI documents regarding DCS 3000 system were made public in 2007. It became clear that the technology employed astonishingly poor security.

Authentication technology was insecure. Well after industry and the military had opted to use hardware tokens for secure authentication to secure networks, DCS 3000 relied on passwords for authentication.[156] Some privileged users shared passwords, removing any capability for adequate system auditing.[157] Remote login was done in the clear, that is, unencrypted.[158]

Auditing systems were similarly primitive. In particular, an FBI security audit had noted, "There were no documented procedures for the retention or review of audit logs."[159] Audit records could be overridden, potentially losing data tracing user activity. It would have been easy for an insider, such as a Kim Philby or Robert Hanssen, to hide traces of nefarious behavior.

In light of the security weaknesses of DCS 3000, these proposals for requiring that the J-standard include robust controls and tamperproof auditing for CALEA-compliant switches are entirely appropriate. It is also appropriate to require that CALEA-compliant switches be subject to rigorous penetration testing.

The engineering specifications of CALEA-compliant switches will require greater specificity, that is, the J-standard will have to describe the architectures of these switches with much greater precision. This will mean less variability in certain parameters than there had been. Putting such requirements in will be problematic, because as new technologies become available, architectures will change, and they will change rapidly.

The requirements of greater specificity in the J-standard run contrary to the technical requirements of innovation. Another way to put this is that there is a stark conflict between the flexibility needed to enable innovative architectures and the tightness of engineering specifications required to ensure CALEA-compliant switches are secure. In this paper, I have argued strongly that the latter is critical (and thus forces the former). But the security for the surveillance mechanisms clearly comes at a high cost.

The ICDs will have to be designed with greater rigor. Implementations should be subject to testing.

---

156. FBI, DIGITAL COLLECTION SYSTEM NETWORK SYSTEM SECURITY PLAN, 15 (2004).

157. *Id.*

158. ACCREDITATION UNIT, FBI, DATA COLLECTION SYSTEM 3000: SYSTEM SECURITY PLAN RISK MANAGEMENT MATRIX, INFO. ASSURANCE SECTION 4 (2006).

159. FBI, CONTROLLED INTERFACE 100: SECURITY EVALUATION REPORT FOR THE DCS 3000, INFO. ASSURANCE SECTION, 4 (2003), *available at* https://www.eff.org/sites/default/files/filenode/061708CKK/073007_dcs03.pdf.

Note that none of these changes require a change in the law. Rather, they require that the FCC enforce the law *as it is currently written*, namely to "ensure that any interception of communications or access to call-identifying information effected within its switching premises can be *activated only in accordance with a court order and with the affirmative intervention of an individual officer or employee of the carrier acting in accordance with the regulations prescribed by the Commission.*"[160]

One result of making the J-standard more prescriptive and of requiring frequent penetration testing of CALEA-compliant switches (and patching of any uncovered vulnerabilities) will be that the implementation costs for CALEA-compliant switches will rise. But that is quite appropriate. In point of fact, this is actually only a cost shifting from the downstream users who would be affected by a breached switch to the developers of the communications switch. That cost shifting is entirely appropriate. Since the costs of economic espionage are so high, it is also appropriate that the changes I recommend are likely to be less expensive in the long term.

As a thought experiment, in designing a robust interception collection system, one could imagine interception at CALEA-compliant switches could require authorization from a judge and an investigator,[161] with both judge and law-enforcement investigator using hardware tokens for authentication. Such a model would provide the clear benefit of active judicial participation to begin interception.[162] But wiretap law allows wiretapping in emergency situations without a judicial order, and any technology for wiretapping would have to accommodate that flexibility.[163] In particular, the switch would need the ability to allow emergency surveillance without a court order. In these cases, if a court order is not forthcoming within the specified time period – forty-eight hours for Title III investigations and seventy-two hours for FISA cases – the collected evidence cannot be used and an audit record must be made of the failed compliance action.

Thus, we have a complicated situation. If CALEA-compliant

160. 47 U.S.C. § 1004 (2010) (emphasis added).

161. Currently the investigator receives authorization from a judge; he presents this authorization to the service provider.

162. Had this been used by the FBI in obtaining telephone records, it is unlikely that the exigent-letter abuses would have occurred. This unauthorized surveillance included private data supplied without a written request, lack of specific data on a request (e.g., dates missing), requests for exigent data when the request was not an emergency. A Review of the FBI's Use of Exigent Letters and Other Informal Requests for Telephone Records, Op. Inspector Gen. 44-53 (2010).

163. This is permitted under the Electronic Communications Privacy Act for wiretaps, pen register, and trap-and-trace device installation in cases of organized crime, an immediate danger of death or serious injury to any person, or a threat to national security. 18 U.S.C. § 2518(7) (2006). For FISA investigations the limit is seven days. 50 U.S.C. § 1805(e) (2006).

switches were to allow emergency overrides, who would ensure that the collected evidence is handled as required by law? The switches themselves could not[164] – and the attendant result might be less oversight, rather than more. This example illustrates what Petroski has observed, "[r]emoving human operators can lead to a well-established pitfall known as the Automation Irony. Because designers can typically reduce but not eliminate the need for human intervention, such efforts frequently make things worse. That's because engineers generally automate the tasks that are easy, leaving the hard jobs for people."[165]

This thought experiment demonstrates the CALEA problem in a nutshell. On the one hand, there is an attraction to further increase security of the system by increasing the robustness of its controls, but on the other, it may create greater complexity. Such complexity is always the bane of security.

That does not mean that one could not design the CALEA-compliant switches to require authorization from both a judge and a law-enforcement investigator before beginning interception. Instead it means that if increased automation is desired, the design specifications must enforce the expected but also the unexpected (e.g., emergency wiretaps without a court order), add bounds – forty-eight hours for emergency Title III taps and seventy-two for emergency FISA collections – and controls to delimit the unexpected situations. One has to design for a world "that's out to get you," and where the attackers may be your own people as well as outsiders.

Heretofore, I have not discussed who might write the security requirements for the new J-standard. The fact is that the government is not currently set up for such an exercise.[166]

It is easier to describe who might not than who might. The FBI and the FCC have been involved in CALEA, the former in developing the J-standard, the latter in its implementation. But their lack of attention to the security risks indicates, at minimum, a lack of expertise. It may indicate more. As I have written elsewhere, "[t]he bureau is a crime-fighting agency. In that guise, the FBI appropriately seeks to use communication interception during investigations . . . It is not in the FBI's investigative interest to publicize weaknesses in communications infrastructure that

164. One way the switch could do so is by sending a message to the judge requiring to whom the wiretap request was made to inform him that wiretapping had taken place under exigent circumstances. Then the judge would set policy into play to ensure that the wiretapped communications were not used in any way. The CALEA-compliance part of the switch would have to be architected to require the judge's name even if the wiretapping was done under exigent circumstances.

165. PETROSKI, *supra* note 54, at 59.

166. Some of this argument appeared earlier in LANDAU, *supra* note 12, at 243-46.

allow the bureau to deploy its various investigative tools."[167] The FCC is not a communications-security shop. Developing that expertise in house would be a major diversion from the commission's primary role of ensuring public access to communications at reasonable cost.

Another candidate might be the Department of Homeland Security (DHS). The original Senate bill proposing the DHS sought to move the National Institute for Standards and Technology's Computer Security Division (CSD) into the new department.[168] Since the passage of the Computer Security Act in 1987, CSD has been responsible for computer security standards, including cryptography, for non-national security – civilian – federal agencies.[169] The division had a rocky existence for its first dozen years as it dealt with conflicting agendas from NSA and industry (there was also evidence of bureaucratic infighting). But by the early 2000s, CSD had developed good working relationships with the computer industry. The proposal to move the division to the new department concerned the industry, which worried that the presence of law-enforcement agencies in DHS might disrupt the progress that CSD and NIST had made in establishing good working relationships (recall that the 1990s had been a time of dispute over public cryptographic standards). While DHS does have a role in cyber-security, it is closer to *applying* security mechanisms to cyberspace *than developing* the fundamental standards.[170] CSD stayed at the National Institute for Standards and Technology (NIST).

Subsequent to this, funding for the Computer Security Division was increased.[171] CSD nonetheless remains a small division focused on federal civilian agency concerns rather than broader societal cyber-security efforts; the non-national security federal agencies are, after all, its charter. The division is certainly not in a position to provide the standards needed for securing complex telephone switches.

The government agency with expertise in communications security is NSA. The problem is that NSA does not have direct authority for aiding non-national-security federal agencies such as the FCC. Instead, a non-national-security agency seeking help from NSA on computer or communications security must first request aid from NIST. Then, with a NIST recommendation, can request aid from NSA (or contractors that NSA had approved). This model fails in the situation of developing or

167. LANDAU, *supra* note 12, at 245.

168. Homeland Security Act of 2002, S. B. 2974, 107th Cong. § 202 (2002).

169. Computer Security Act of 1987, Pub. L. No.100-235, § 20 (1988) (repealed 2002).

170. *See, e.g.*, Homeland Sec. Presidential Directive 7: Critical Infrastructure, Identification, Prioritization, and Protection, Pub. Papers §§16, 22(c) (Dec. 17, 2003).

171. *See generally* INFO. SEC. & PRIVACY ADVISORY BD., THE NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY COMPUTER SECURITY DIVISION: THE CASE FOR ADEQUATE FUNDING (2004). Disclosure: I was a member of that advisory board.

regulating implementation a secure standard for CALEA-compliant switches.

This is clearly a serious gap in protecting civilian communications systems. This is not to say that there aren't efforts by non-national-security agencies to develop secure computer or communication systems. The FCC and DHS are heavily involved in ensuring that emergency systems work during national crises. NIST's Computer Security Division provides guidance for some aspects of securing communications.[172] But the heavy work of threat modeling and penetration testing against communication networks is still done only on the national-security side of the house. The failure of the FCC to consider communications security on CALEA-compliant switches, and the importance of secure communications to the U.S., raises the issue of whether there should be the equivalent of an NSA IAD in the civilian sector – or whether IAD should perhaps move to the non-national security side of the government, with both a classified and non-classified side of the house.[173]

B. Ensuring Interception Standards Remain Secure

When CALEA was passed in 1994, attacks against CALEA-compliant switches were likely to be mounted by the targets of the switches – organized crime, drug dealers, etc. – and by those who were seeking free services. Security focused on network reliability and those seeking free services. Neither the Department of Justice nor the Department of Defense anticipated the essentially continuous more general cyber-security attacks that now constitute a serious economic threat against the United States.[174]

This shift is illustrative of one of the problems with threat modeling: threats change. Threats change, and the motivation and capabilities of the attackers change. Technology also changes – and not just the technology under the control of the service provider changes. As that occurs, new and different attackers, with different capabilities, emerge.

What this means is that the previous threat modeling is no longer

---

172. The Computer Security Division provides guidance in implementing secure modes of communication. *See e.g.*, NAT'L. INST. OF STANDARDS AND TECH., GUIDE TO SECURING WIMAX WIRELESS COMMUNICATIONS 800-127 (2010); NAT'L. INST. OF STANDARDS AND TECH., GUIDELINES ON CELL PHONE AND PDA SECURITY 800-124 (2008); NAT'L INST. OF STANDARDS AND TECH., GUIDE TO GENERAL SERVER SECURITY 800-123 (2008). While the material covered is technical, one can broadly categorize the guidance work as recommendations for secure implementation rather than for secure development of the technologies.

173. This last suggestion of moving IAD to the non-national-security side of government was made by Mike Jacobs, former director of the IAD.

174. Lynn, *supra* note 19, at 98-99; OFFICE OF THE NAT'L COUNTERINTELLIGENCE EXEC., FOREIGN SPIES STEALING U.S. ECONOMIC SECRETS IN CYBERSPACE: REPORT TO CONGRESS ON FOREIGN ECONOMIC COLLECTION AND ESPIONAGE 4 (2011).

valid. A switch that was deemed secure in January can no longer be assured of being secure in June, and the testing that was done in January must be done again, modified with new knowledge. Given the complexity of the switch environment, performing penetration testing on deployed switches every six months is not unreasonable.

This is a partial answer. I have said penetration testing, but I have not described the skill level of the attackers. In fact, what level of penetration testing is appropriate for CALEA-compliant switches is not a subject for this paper (and is, indeed, likely to change over time). But that penetration testing of CALEA-compliant switches should be performed twice annually regardless of whether there have been major changes in the switch is in scope. And it is a recommendation that I cannot make too strongly.

C. Securing Critical Infrastructure in the Face of Changing Threats

In this paper, I have observed that the security risks of CALEA-compliant switches are at best extremely problematic and most likely completely untenable in a society beset by cyber-security threats. I have proposed that the standards for CALEA-compliant switches include far more robust authentication requirements, stronger auditing mechanisms, and strong controls on remote delivery of content. I have recommended semiannual threat modeling and penetration testing be required for all CALEA-compliant switch deployments.

These observations have broader application than CALEA-compliant switches, of course. In large part, critical infrastructure has been built to withstand natural phenomena, not targeted attacks. Prior to adoption, critical infrastructure should undergo a study of the long-term implications of security risks. Developing the appropriate models requires not only engineering, but also includes evaluating relative risk and cost. In a world of changing threats, this broader scope of evaluations is necessary.

But let us not get too general. Just as houses in North Carolina are not built to withstand a Category 5 hurricane, and homes in San Francisco not built to withstand a magnitude 9 earthquake, critical infrastructure should not be built to protect against any conceivable threat. But because the centrality of electronic communications to public discourse, commerce, political, and public and private life cannot be underestimated, neither should the importance of the security and privacy of these communications.[175] It is critical to secure communications

175. I should note that although steps taken to increase security of society often come as the expense of privacy of individuals that is not the case in the solutions proposed in this paper. Ensuring that interception is done securely in CALEA-compliant switches increases

infrastructure. The government has a strong responsibility to ensure that its interception standards increase security rather than putting it at greater risk.

both society's security and individuals' privacy.