Security, Liberty, and Electronic Communications

Susan Landau

Sun Microsystems, email: susan.landau@sun.com

Dedicated to the memory of Dorrie Weiss.

1 Introduction

We live in perilous times. We live in times where a dirty bomb going off in lower Manhattan is not unimaginable. We live in times where the CIA interrogations of al Qaeda leaders were so harsh that the FBI would not let its agent participate [36]. We live in times when security and liberty are both endangered.

We also live in times of unimaginable technical creativity. It is faster to use Instant Messaging to query a colleague halfway across the world than it is to walk down the hallway and ask the question, when Google can search four billion web pages faster than the time it takes to pull the right volume of the Oxford English Dictionary off the library shelf. We live surrounded by a plethora of communicating and computing devices — telephones, PDAs, cell phones, laptops, PCs, computers — and this is only the beginning of the communications revolution.

September 11th presaged a radical change in terrorist intent, a radical change that few had anticipated. The U.S. government responded to September 11th in a number of ways, including the passage of the U.S.A. Patriot Act, which qualitatively extended the government's electronic-surveillance capabilities. The Patriot Act engendered strong debate (though not in Congress, where the law passed handily). The most controversial issue regarding the changes in electronic-surveillance law was that the requirement that foreign intelligence be a "primary" reason for a Foreign Intelligence Surveillance Act (FISA) wiretap was modified to foreign intelligence need only be a "significant" reason for a FISA tap.

Absent from the debates on the Patriot Act was an acknowledgement of the radical changes that had occurred in communications technologies since the passage of the first Federal wiretap statute in 1968. Communications technology has changed in numerous ways over the past forty years — there is now wide availability of mobile communications, a vast increase in connectivity, and packet-switched systems are being employed for telephony — but there has been no commensurate review of electronic-surveillance laws. We are in a peculiar state: we communicate using mobiles phones and laptops, but the laws governing electronic surveillance were developed at a time of fixed-location circuit-based switching systems. Instead of a full-scale reevaluation of surveillance laws, over the last two decades we have pursued a path of minor tweaks to the electronic-surveillance laws. The result is an electronic-surveillance regime that may be well out of sync with the times. This has serious implications for security, liberty, technology, and innovation. In this paper, we examine electronic-surveillance laws in light of current threats and new technologies. We begin by examining the climate in which wiretap laws came to be enacted.

2 The Political Climate at the Time of the Wiretap Act

The sixties were a time of turmoil in the United States, a time of political protest, and civil unrest. In 1963, President John Kennedy was assassinated in a motorcade in Dallas, Texas. In 1965 Malcolm X was killed as he delivered a speech in an auditorium in Harlem. In April 1968, Martin Luther King was killed, and two months later, Robert Kennedy, who was running for President, was shot moments after he learned he had won the California primary. There had been civil rights marches in Washington in the early 1960s, and anti-Vietnam protests in the latter half of the decade. In the summer of 1964, downtown Newark burned; in 1965, the Watts section of Los Angeles; in 1967, downtown Detroit.

It was against this backdrop that the President's Commission on Law Enforcement and Administration of Justice presented its report. Organized crime had been a problem in the United States since Prohibition, but, because FBI Director J. Edgar Hoover ignored it, so did the Federal government. Several events in the late 1950s and early 1960s changed that.

The first was the discovery, on November 15, 1957, by a New York state trooper, of a meeting of organized crime bosses. The trooper was doing routine morning rounds when he discovered far too many black limousines for the tiny upstate town of Apalachin. The trooper set up a roadblock; the crime bosses fled, and "the next day, the nation awoke to headlines like 'Royal Clambake for Underworld Cooled by Police,' and 'Police Ponder NY Mob Meeting; All Claim They Were Visiting Sick Friend' [13, pp. 168-9]. Meanwhile, while counsel to the Senate Select Committee on Improper Activities in the Labor or Management Field, Robert Kennedy had uncovered ties between the unions and organized crime. When he became attorney general, Kennedy made organized crime a priority [29]. And finally, an organized crime turncoat, Joseph Valachi, broke the code of silence by testifying to a Senate investigating committee in 1963.

This confluence of events made pursuing organized crime a law-enforcement priority in the late 1960s. The complications of investigating organized crime — the reluctance of victims to testify, so-called victimless crimes (e.g., prostitution), and the corruption of local law enforcement made electronic surveillance a particularly valuable tool. The Commission concluded, "A majority of the members of the Commission believe that legislation should be enacted granting carefully circumscribed authority for electronic surveillance to law enforcement officers..." [33, p. 203].

But, as noted in [13, p. 170],:

> Not all experts agreed with the commission's conclusions. Attorney General Clark prohibited all use of wiretaps by federal law-enforcement of-

> ficers. He told Congress: 'I know of no Federal conviction based upon any wiretapping or electronic surveillance, and there have been a lot of big ones. ... I also think that we make cases effectively without wiretapping or electronic surveillance. I think it may well be that with the commitment of the same manpower to other techniques, even more convictions could be secured, because in terms of manpower, wiretapping, and electronic surveillance is very expensive." [8, p. 320] Clark pointed out that in 1967, without using wiretaps, federal strike forces had obtained indictments against organized-crime figures in nine states, and that "each strike force has obtained more indictments in its target city than all federal indictments in the nation against organized crime in as recent a year as 1960" [8, pp. 79-80]

President Johnson publicly supported Clark's opposition to wiretapping, and the President proposed limiting wiretapping to national-security cases [9, p. 222]. But political turmoil and the Crime Commission's report led Congress in a different direction, and in 1968 it passed the Omnibus Crime Control and Safe Streets Act of 1968 (18 USC §2510–2521), Title III of which legalized law-enforcement wiretaps in criminal investigations. Because of the very invasive nature of the search, wiretaps were limited to a list of twenty-six crimes specified in the act, including murder, kidnapping, extortion, gambling, counterfeiting, and sale of marijuana. The Judiciary Committee's report explained that "each offense was chosen because it was intrinsically serious or because it is characteristic of the operations of organized crime," [44, p. 97].

President Johnson was ambivalent about wiretaps. He had used them — on Martin Luther King during the Democratic convention in 1964 and on Vice President Humphrey in 1968 — but the President described the Title III provisions for wiretapping as undesirable [9, p. 1842]. Nonetheless Johnson signed the bill. Because of the invasive nature of electronic surveillance, Congress decided that there should be stringent oversight, and that review of a federal wiretap warrant application must be done by a federal district court judge.

The judge must determine that (i) there is probable cause to believe that an individual is committing, has committed, or is about to commit an indictable offense; (ii) there is probable cause to believe that communications about the offense will be obtained through the interception; (iii) normal investigative procedures have been tried and either have failed, appear unlikely to succeed, or are too dangerous; and (iv) there is probable cause to believe that the facilities subject to surveillance are being used or will be used in the commission of the crime (§2518 (3)(a-d)).

Title III covers procedures for obtaining wiretaps for law-enforcement investigation. In 1972, in a court case involving "domestic national-security issues," the Supreme Court ordered an end to warrantless wiretapping, even for national-security purposes. Because of Watergate, and the discovery of numerous so-called national-security wiretaps that were actually wiretaps for political purposes [42], it took until 1978 before Congress was actually able to frame and pass legislation authorizing procedures for obtaining wiretaps for national-security investigations: the Foreign Intelligence Surveillance Act. The judge, a member of the Foreign Intelligence Surveillance Court, a court of eleven judges appointed from seven of the United States judicial circuits (§1803 (a)), must determine (i) that there is probable cause that the target is a foreign or target of a foreign power, (ii) that there is probable cause that the targeted communications device is being used by the foreign power or its agent, that (iii) that a primary purpose of the surveillance is to obtain foreign intelligence information, and that (iv) such information cannot reasonably by obtained by other investigative techniques. [1]

Title III and FISA form the basis for U.S. wiretap law. There are also state statutes (approximately half of all criminal wiretaps in the United States are done under state wiretap warrants). The rules governing state wiretaps must be at least as restrictive as those governing Title III.

There have been several updates and modifications to the federal wiretap statutes, which will be discussed after examining the changes in communications technology over the last four decades.

3 Current Threats

In the U.S. we are currently seeing a strident debate on surveillance technologies, most especially datamining. This paper is not the place for a full discussion of the methods and means used in terrorist investigations. In the context of reexamining electronic-surveillance laws, however, it is useful to make some observations about terrorism and terrorist investigations.

By any measure, terrorism is a very difficult offense to investigate or prevent. In many cases, the first crime committed is the only crime. There is no trail. The investigative reporter, Seymour Hersh, described CIA efforts in southern Lebanon during the 1980s,

> . . . when the C.I.A. started to go after the Islamic Jihad, a radical Lebanese group linked to a series of kidnappings in the Reagan years, 'its people systematically went through documents all over Beirut, even destroying student records.'

One of the hallmarks of modern terrorist groups is the shifting and diffuse organizational structure [39, p. 271]. On the one hand, this means that eliminating the leadership does not necessarily eliminate the problem. On the other, diffuse and ever-changing structures create weaknesses within the organization. One that can be exploited is the terrorists' need for communication.

In this situation, traffic analysis often proves more useful than wiretapping. Wiretaps can be confused by encryption, even encryption of a very simple sort. Seymour Hersh reported that,

[1] The law provides that "[N]o United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States" (§1805(a)(3)(A)).

> The terrorists coped with the American ability to intercept conversations worldwide by constantly changing codes — often doing little more than changing the meanings of commonly used phrases.

The problem is being unable to decode the language is not new. It can even occur without deliberate intent by the criminal or terrorist group. The National Research Council report, *Cryptography's Role in Securing the Information Society* described an FBI wiretap of police officers who were allegedly guarding a drug shipment. The FBI agents overhead a conversation in which the officers discussed murdering an individual who had filed a police brutality complaint. The bureau was unable to decode a participant's "street slang," and was thus unable to prevent the murder [10, p. 88].

The inability to understand surveilled conversations does not mean that the surveillance is useless. In particular, traffic analysis has become an extremely valuable aspect of surveillance, and one cannot confuse traffic-analysis efforts in quite the same way as one confuses content analysis. One example of the value of traffic analysis is that Osama Bin Laden stopped using a cell phone in late 2001 because of the tracking capabilities of U.S. intelligence.

Even "anonymous" cellphones can be used for tracking. In a case in 2002, investigators tracked al Qaeda members through terrorists use of prepaid Swisscom phonecards. These had been purchased in bulk — anonymously. But when investigators discovered through a wiretap on an intercepted call that "lasted less than a minute and involved not a single word of conversation" that they were on to an al Qaeda group, the agents tracked the users of the bulk purchase [45]. The result was the arrest of a number of operatives and the break-up of al Qaeda cells. You can run, but you can't hide. Anonymity is not all that it is cracked up to be.

One important aspect of terrorist investigations is to "follow the money." Many terrorist groups hide behind legitimate charitable groups, but these are groups with money trails [39, p. 274]. (We should note, however, that "following the money" is not a straightforward issue in terms of civil liberties. The Patriot Act section dealing with money laundering and terrorist financing is controversial admidst claims that its provisions have been applied to charitable groups with no ties to terrorist activities.) Money trails can be complicated to follow, and the terrorists do a good job of hiding trails by passing money through many intermediaries, but the fact is that there is a trail. Once there is trail, it can be investigated.

The current terrorist threat is very different from earlier terrorist movements. A different from earlier terrorism threats, such as the Russian nihilists of the nineteenth century or the Palestinian terrorists of the 1970s, is the huge reservoir of potential recruits. Globalization complicates the problem. (Indeed, one legitimately argue that globalization is a large part of the problem — but that is a topic for a different paper.) In the late 1990s, Senators Hart and Rudman chaired a national security commission study to examine emerging threats. In a prescient observation, the Hart-Rudman report in early 2001 warned of the likelihood of catastropic domestic attacks caused by international terrorism. The report observed, “All borders will become more porous.” [41, p. 2] This has already happened in Europe. While the borders have become porous, apparently cooperation between different nations' law enforcement has not yet followed suit.

Terrorism is not a passing phenomenon. It will be with us for a long time. It is important that we respond to the threat in a way that simultaneously protects our security and our liberty.

4 Changing Communications Technology

The first hundred of years the telephone saw change: from local systems entirely mediated by operators to global networks entirely run by electronic switching systems. There was innovation: mobile phone, first deployed n 1946 [6, 215], faxes, and modems. There was development of infrastructure: optical fibers and communication satellites, as well the digitization of the backbone network.

Yet slightly more than a generation ago, the telephone remained a fixed device: a black machine with a rotary dial that transmitted voice (also data; from the beginning, the telephone was also a data-transmission network data, e.g., telegraph). In the sixties innovation was the introduction of the “Princess” phone (in colors!: white, beige, pink, blue, or turquoise) and Touchtone service (buttons instead of rotary dials), while industry got Centrex, an automatic switching exchange for large offices, and “data-phones” (modems) [6, p. 266]. What occurred in the first century was growth: ten million phone users in 1900, one hundred million in 1960, five hundred million in 1990[2].

The innovation of the first hundred years of the telephone pales in contrast to the growth and changes of the last decade and a half. There were 1.4 billion users in 2000, 400 million of those cell phone users. There probably has been as much innovation in telephony in the last quarter century as there had been in the previous one hundred years.

Recent telecommunications growth has been spurred by three technical developments: mobile technology, greater bandwidth, and the Internet. AT&T has had car phones since 1946 [6, p. 215], but such service was rare and expensive until the early 1990s. Mobile technology took off with the 1983 development of “cell” technology. In under a decade, cell phones have become ubiquitous, as has the wireless Internet. Once the Web appeared, the race to install broadband was on. In 1999, less than 10% of U.S. households had broadband; by early 2004, the percentage was 45% [32]. The shift to Internet communications is the most fundamental of the changes. The Internet enabled email, (which is the killer app of the Internet) [34], Instant Messaging, and the nascent technology: VoIP (voice over IP).

This is only the beginning of the communications revolution. We are moving from a circuit-based system based on transmitting voice to a high-speed, packet-switched network transmitting data. The pervasiveness of our communication systems will shift all that we do. These social and technological changes should be taken into account the discussion of electronic-surveillance laws.

[2] These numbers are international.

5 The 2004 Questions

5.1 What is the Current Legal Framework?

Title III and FISA set the framework for U.S. electronic-surveillance laws. Since their passage (in 1968 and 1978 respectively), there have been three major Federal laws that affected wiretapping: the Electronic Communications Privacy Act (ECPA), the Communications Assistance for Law Enforcement Act (CALEA), and the U.S.A. Patriot Act.

ECPA updated Title III and FISA to apply to "electronic communications," defined as communications carried by wire or radio and not involving the human voice. ECPA was less strict about the type of crimes for which there could be interception: any federal felony may be investigated using interception of electronic communications. ECPA also modified the rules for electronic communications. In contrast to Title III and FISA, which required naming the device and person to be tapped, ECPA allowed for "roving wiretaps" — wiretaps with unspecified locations — if there was demonstration of probable cause that the subject was attempting to evade surveillance by switching telephones. In recognition of the greater ease in obtaining signalling information, ECPA provided for traffic analysis. Under ECPA, a subpoena is needed for all pen registers, which record all numbers dialed from a phone, and all trap-and-trace devices, which record all numbers dialed to a phone. Furthermore, under ECPA, law enforcement only needs a search warrant, rather than the more stringent wiretap warrant, to access stored communications (voice mail or email that has been read and then stored).

The Communications Assistance for Law Enforcement Act (CALEA) in 1994 was very controversial. In 1992 the FBI pressed for a "Digital Telephony" bill, which required that all telephone-switching equipment be designed to accommodate wiretapping. Civil-liberties groups and the telecommunications industry opposed the bill, and there were no sponsors of it.

The FBI returned to Congress in 1994 with a modified version, the "Communications Assistance for Law Enforcement Act," which included a $500 million authorization (but not appropriation) to the telecommunications companies for modifications to old equipment (this caused the telecommunications companies to drop their opposition). The bill required that any equipment deployed after January 1, 1995 would have to meet law-enforcement interception standard; the Department of Justice would determine which would be the standards-setting organization. This bill passed in the waning days of 1994 after certain civil-liberties groups dropped their opposition.

From the start, implementation of CALEA went badly. The Department of Justice put the FBI, an agency not known for expertise in telecommunications, in charge of setting the implementation standards. In October 1995 the FBI announced its requirements, which would have entailed capacity to simultaneously monitor thirty thousand lines [19] [20] [13, p. 197], a striking number at a time when the total number of annual Title III and FISA surveillances, including pen registers and trap-and-trace devices, was a quarter of that. (In 1995 the average Title III wiretap ran for 29 days [1, p. 13]. There is no public information about the length of FISA taps.) There were strong objections to the methodology the FBI used to arrive at this figure and the bureau decided to reexamine the capacity issue. Their new methodology required capacity to run sixty-thousand surveillances simultaneously[3] [20][13, p. 198]. Recognizing that the delay in developing compliance standards made it impossible for the telecommunication companies to meet the law's deadline (October 1, 1998, four years after the passage of CALEA), the FCC granted an extension til June 2000 [22].

There was also a fight about location information for cellular calls. During hearings on CALEA, FBI Director Freeh had promised that the bill would not expand wiretapping powers[24, p. 29], and the legislative report stated that "call-identifying information shall not include any information that may disclose the physical location of the subscriber" (CALEA §103 a2B). Nonetheless the FBI proposed that the cellular telecommunications group adopt a standard that would enable law enforcement to quickly establish the location of a wireless user [30]. In a 2000 decision, the U.S. Court of Appeals upheld the location standard implemented as a result of CALEA (*United States Telecommunications Association et al. v. FCC and U.S.,* 99-1442, U.S. Court of Appeals).

In CALEA, Congress defined "information services," distinguishing it from "telecommunications services." Information services were defined as "(A) mean[ing] the offering of a capability 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 telecommunications network" (CALEA §102 (6)). The bill explicitly states that the interception requirements do *not* apply to information services (CALEA §103 (b)(2)(A)).

Over time, the list of crimes for which Title III is applicable grew substantially. It now lists 98 offenses, including computer fraud and abuse (18 U.S.C. §2516). Even though the vast majority of wiretapping investigations concentrate on drug trafficking and organized crime[2, Table 3], the law is not so tightly focused as had been at its inception.

5.2 How Exposed is Personal Information?

Changes in technology as well as social norms means that individuals leave tracks wherever they go in modern society. A generation ago, individuals scrawled their names on a card inside the book they borrowed from a library; now book borrowing records library are entered into a central database. A generation ago, individuals received a hotel key; now the "key" is a plastic card that includes a

[3] In both cases, the proposed monitoring capacity appears as a percentage of phone lines. Thus, if number of phone lines increases, required monitoring capacity would do so proportionally.

strip that may or may not have the lodger's name and credit-card information on it. A generation ago, an individual gave a name for a plane ticket, and then may have sold the ticket to a friend; now the name on government-issued IDs must match name on the the ticket. As Jeffrey Rosen has observed, we are the "naked crowd" [37].

One significant change over the last several decades is the major loss of anonymity that has resulted from credit cards becoming the payment method of choice. The financial dossiers created enable tracking and identification of individuals in a way that plunking three hundred dollars down for a used car does not. Because credit cards have essentially become required for travel (at least for car rental and hotel reservations), credit-card records provide excellent after-the-fact records of where individuals have been, when (and, in some cases, with whom). Evidence of this is in the tracking of the September 11th hijackers. By September 14, 2001, law enforcement had put together a impressive dossier on the hijackers: where and how they had purchased their tickets, where they were living before the attacks, and where they had gone to and flight school (not all of them had) [23]. It was in the ubiquitous trail that individuals leave as part of modern life.

We leave video tracks not just at the airport and the ATM, but at totally unexpected stops. Timothy McVeigh had no intention of leaving a trail when he rented a truck in Junction City Kansas but, as noted in [13, p. 267], he had.

> Investigators ...used photos from several days before the explosion to prove that Timothy McVeigh was the "Robert D. Kling" who, on the afternoon of April 17, 1995, in Junction City, Kansas, rented the Ryder truck used in the bombing. Days and weeks after the bombing investigators meticulously reconstructed McVeigh's movements on April 17. Surveillance photos taken at a McDonalds about a mile from the Ryder agency showed McVeigh at the restaurant at 3:49 and 3:57 PM on that day. Shortly afterward, "Kling" rented the truck. When prosecutors claimed that the McDonalds's photo was of McVeigh, his lawyer did not dispute the point. The photo was taken several days before there was any hint it would be useful in a criminal case —and *then the evidence was available when needed*[5].

Imminent changes in technology will create even more detailed trails. Sensors, low-cost wireless devices, will monitor the environment and report back: "The elderly patient has a blood pressure of 110/70," "The room is at 75 degrees." RFID (Radio Frequency ID) devices will report about items an individual carries on his person: clothes, currency, a book. The sensor and RFID communications will often occur without the individual's knowledge[4].

It is not clear how an expiring milk carton informing the supermarket that it is time for a new dairy order will benefit tracking of terrorists and criminals. But one wouldn't necessarily have anticipated that an intercepted phone call in which no words were spoken and that was paid for via an anonymously-purchased

[4] The Internet will be the communications medium.

prepaid card would have led to a major breakthrough in a terrorist investigation either. The fact that data storage is dropping in price encourages the storage of transactional information, information that will be accessible to investigators.

It is not currently the case that an individual's data is arbitrarily subject to law enforcement perusal. The question of under what circumstances government can do data mining is currently a subject of much debate and some studies (e.g., [40]). In thinking about federal wiretap statutes, it is important to put the issue in context, and in particular to be cognizant that there is much more data easily accessible on individuals than there was at the time of the passage of the Wiretap Act. Under appropriate circumstances, that data is available to law-enforcement and national-security officials.

5.3 What is the Effect of Communications Surveillance on Liberty?

We have briefly examined the changes in communications technology and in the accessibility of individual's private data at the dawn of the twenty-first century. We need to begin at the beginning, the time of the founding of the United States. As Whitfield Diffie has remarked,

> [P]rior to the electronic era conversing in complete privacy required neither special equipment nor advanced planning. Walking a short distance away from other people and looking around to be sure that no one was hiding nearby was sufficient. Before tape recorders, parabolic microphones, and laser interferometers, it was not possible to intercept a conversation held out of sight and earshot of other people. No matter how much George III might have wanted to learn the contents of Hancock's private conversations with Adams, he had no hope of doing so unless he could induce one or the other to defect to the Crown[13, p. 2].

In the United States, the founders reacted to the broad searches by British solders under general writs of assistance by restricting government power through the Fourth Amendment of the U.S. Constitution,

> The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures shall not be violated, and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

"No warrants shall issue but upon probable cause ...and particularly describing the place to be searched, and the persons or things to be seized." This would be significant when it came time to apply the Fourth Amendment to communications surveillance. Justice Louis Brandeis wrote in his famous dissent in the Olmstead case,

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is

> invaded, and all conversations between them upon any subject, and although proper, confidential, and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call, or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping [4, pp. 475-6].

Experiences with government surveillance, extensively described elsewhere (see e.g., [13, pp. 137-150, 172-179, 271-2], [42], demonstrated serious dangers to political discourse and public expression. During the period from the 1940s to the 1970s, for example, Supreme Court justices, White House staffers, members of the National Security Council, Congressional staffers, civil-rights leaders, including Martin Luther King and Ralph Abernathy Jr, anti-Vietnam War protesters, and journalists were wiretapped. These breaches made Congress wary of providing law-enforcement and national-security investigators with such a potentially invasive tool. This is why the requirements for a wiretap warrant are significantly more stringent than those for a "normal" search warrant [5].

Wiretaps intrude on a conversation between two people and thus require the high level of wiretap search warrant before tapping can commence. But there is no similar level of protection for transactional information on what number is being called and what number is calling. The legal rationale is that such transactional information is already being shared with a third party (in this case, the telephone switch) and the communicating parties do not have any expectation of privacy on the data. Thus a subpoena, which can be obtained from a magistrate, suffices for pen registers and trap-and-trace devices[6].

[5] It is also why public reporting of Title III wiretaps is required; each year, the Administrative Office of the U.S. Courts produces a report listing each Title III wiretap of the previous year (ongoing taps are not reported until they have ceased to be used), including the D.A., the judge issuing the wiretap search warrant, the length of order, the "most" serious crime for which the wiretap was ordered (there may be more than one for a single wiretap), the number of incriminating and non-incriminating calls picked up on the wiretap, the cost of the surveillance, etc. (Except for annually reporting to Congress the number of surveillances, there are no public disclosure requirements for FISA wiretaps.)

[6] This paper concentrates on the technology side of the electronic-surveillance issues, not the policy. Nonetheless, we would be remiss if we did not point out that traffic analysis, though usually less intrusive than content surveillance, may nonetheless cause severe privacy breaches. One such example occurred in the 1980s FBI investigation of CISPES, the Committee in Solidarity with the People of El Salvador, an American group which supported the opposition to the El Salvadorian government. On the basis of an informer's information, the FBI started an investigation of CISPES, eventually culminating in files on more than twenty-three hundred individuals. Much of the information was obtained through phone records. The investigation was not justified; the group was not a terrorist organization, and in 1988, FBI Director William Sessions told Congress that, "[T]here was no reason ... to expand the investigation so widely" [38, p. 122].

In this paper we are focusing our discussion on technology implications of wiretapping rather than policy issues. Nonetheless, as we consider the role of surveillance in current communications technology, we must never lose sight of Brandeis's words, "As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire tapping [4, pp. 476]."

6 Telephony and the Internet: Two Different Architectures

The Public Switched Telephone Network (PSTN) was built to maximize the quality of voice transmissions and everything in the network was designed to that end. The Internet was designed for reliability, a very different quality. The PSTN uses circuit switching to transmit information from sender to receiver, the Internet, packet switching. The PSTN and the Internet have fundamentally different architectures. This simple fact means that many of the surveillance tasks do not directly translate from one domain to the other.

6.1 Electronic Surveillance on the Internet

Consider, for example, the effect of packet-based technology on the transmittal of transactional information. In telephony, signaling information appears at the beginning of the call and is separated from call contents. In packet-switched systems such as the Internet, because data is broken into "packets," each one of which has the addressing information, contents do not have the same physical separation from the "signalling" information (probably more properly called transactional information in this case).

Furthermore, electronic communications typically present more personally-identifiable information present in the so-called transactional information. At a minimum, this may simply include place of business, e.g., susan.landau@sun.com. But it may include much more, e.g., if the transactional information is the result of a google search, the URL will reveal the search terms [7].

[7] That "pen registers" and "trap-and-trace devices" garner additional information when used in packet-switching network systems than they do in traditional circuit-switched telephony systems did not escape the notice of technologists and civil-liberties groups. When the news of Carnivore, the FBI's Internet monitoring system became public in the summer of 2000, one of the criticisms of the system was that the transactional information that Carnivore was sweeping up was more than the government was entitled to under the limited subpoena power used for pen registers and trap-and-trace devices. Carnivore was quite controversial. In the summer of 2001, it looked as if there might Congressional action limiting Carnivore's use. Instead September 11th happened. The Patriot Act gave law enforcement explicit power to use subpoenas for pen registers and trap-and-trace devices on electronic communications (§216).

An even more crucial different between the PSTN and the Internet is that in the Internet, *the intelligence is at the endpoints*. The underlying network system is simple, while the endpoints can deploy complex systems. This fundamental architectural idea is what makes the Internet so versatile. Applications can be designed far beyond what the original designers of the Internet had in mind. And indeed, innovation has flourished because the endpoints competed and created new services. No one needs to depend on the infrastructure company to do the innovation for them.

The design flexibility comes at a price that we do not often think of as a price: the Internet is hard to control. This does not mean political or border controls (though those are also often difficult to implement on the Internet) but design control. This is not a bug; it is an extremely attractive feature. In a sharp, and deliberate, distinction from the telephony network, the Internet was designed to be loosely controlled. The layered approach to network design provides that effect and is what has enabled much of Internet innovation.

For those that choose to invest the effort, Internet communications can be fully protected. The Internet design of intelligence at the endpoints complicates wiretapping, which is useless if end systems adequately protect their communications (although a wiretapped encrypted conversation will still provide traffic information). In recent years, protecting the privacy of communications has become an important security goal. Indeed, the U.S. government has moved in the direction of simplifying the deployment of communications security in commercial equipment, partially as a result of the government's move to purchasing COTS (commercial off the shelf) equipment rather than the purchase of custom-designed systems. Instead of restricting the use of cryptography, the U.S. government has recently encouraged a number of security efforts, including the development of the 128-bit Advanced Encryption Standard and the deployment of Elliptic Curve Cryptosystems. Attempts to build wiretapping capabilities into Internet protocols would seem to go against these efforts.

At the same time, as an IETF Network Working Group studying the issue of architecting wiretap requirements into Internet protocols observed, "the use of existing network features, if deployed intelligently, provide extensive opportunities for wireteapping" [35].

6.2 The Risks Wiretapping Poses to Internet Security

Under CALEA, telecommunications systems deployed after January 1, 1995 must be built wiretap accessible. Suppose one were to call for that same requirement on the Internet. Does such an obligation make sense? Can it be architected in? What does it do to security requirements?

Wiretapping is an architected security breach. Saying that Internet communication protocols necessarily must have wiretapping requirements built in is to say that security loopholes must be built into communication protocols. It means that privacy of the communication must be deliberately violated and in a way that does not alert the sender or recipient.

Of course, U.S. law-enforcement and national-security agents are not the only ones interested in wiretapping the Internet; foreign governments are as well. Any technology that is designed to simplify Internet wiretapping by U.S. intelligence may well be exploited by foreign-intelligence services. During the discussions on CALEA, there were concerns about the security problems created by "building in" wiretapping capablities for digital telephony [15]. Such fears pale when measured against designing such capabilities for the Internet. Internet wiretapping technology, found and reverse engineered by foreign-intelligence services, could enable massive surveillance of U.S. "persons" (citizens and corporations). Used in combination with inexpensive automated search technology, this could lead to serious security breaches.

There is risk to the U.S. economy (the potential loss of corporate information). There is risk to U.S. national security (through the provision of cost-effective massive intelligence gathering). There is risk to the freedom of U.S. citizens. These are the risks [7] that the European governments responded to when, in 1999, they decided to liberalize their cryptographic export-control policy. As did the United States when it liberalized its cryptographic export-control policies shortly afterwards [14].

If we were to build access for U.S. law enforcement or national security into Internet communications, such protocol design would have be done very carefully. Can it be? It is highly doubtful. As the IETF Network Working Group observed, any protocol designed with wiretapping capabilities built in is inherently less secure than it would be without the wiretapping capability. Building wiretapping requirements into network protocols makes the protocols more complex. As is well known, complex protocols are prone to security flaws. The secure Internet is a challenge. Despite best efforts, security breaches slip into many protocols. No one wants to see deliberately-architected security breaches. In 2000 the IETF Network Working Group decided not to consider requirements for wiretapping as part of the IETF standards process [35].

7 What is the Right Tradeoff for Communications Surveillance?

What are the costs to communications technology of continuing to enable wiretaps? A recent FBI petition to the FCC gives an illustration. The bureau argued that "CALEA's purpose is to help lawful electronic surveillance keep pace with changes in telecommunications technology as telecommunications services migrate to new technologies" [21, pp. 3-4] and stated that thus "CALEA is applicable not only to entities and services that employ circuit-mode technology, but also to entities and services that employ packet-mode technology" [21, p. 6]. The Bureau urged the FCC to declare that any service providing voice communications, including Voice over IP (VoIP), should be viewed as a "telecommunications carrier."

The breadth of this claim is startling. Were the FCC to grant the petition (unknown at the time of this writing), this would put the FBI squarely in the middle of designing IETF protocols. What would the technological cost of granting this petition be? One can scarcely imagine. At a minimum, granting the petition would "drive up costs, impair and delay innovation, threaten privacy, and force development of the latest Internet innovations offshore" according to a response filed by a coalition of industry and civil-liberties groups [26]. As we have observed earlier, it would also threaten security.

Does the value of wiretapping justify trying to preserve the tool? This, of course, depends on whom you ask. As the FBI was pressing the Digital Telephony bill in the early 1990s, the bureau argued that wiretapping was a critical tool in the fight against organized crime. The FBI presented claims that court-ordered wiretaps resulted in over seven thousand convictions, three hundred million dollars in fines levied, and over three-quarters of a billion dollars in recoveries, restitutions, and court-ordered forfeitures over a six-year period [18]. But White House staffers [3], the Treasury Department [28], and the Vice-President's office [31] all disputed the FBI numbers.

There is no question that wiretapping can be effective in some cases. Its most important value may be as a deterrent: knowing that law enforcement is listening in, criminals and terrorists stay off the line. Or they speak in code: "The big guy is coming. He will be here soon." [45] Making the use of electronic communications difficult for criminals and terrorists denies them one of the greatest technological advances of the last century.

As we have seen, greater surveillance value may come from traffic analysis, which has already shown remarkable benefits in the fight against terrorism. Given the U.S. government's shift on cryptographic export controls, one might reasonably argue that intelligence agencies have come to the same conclusion.

The debate about electronic surveillance must not occur in isolation. U.S. wiretapping laws were passed when the opportunity to easily obtain massive, automatically-created, data trails did not exist. Video cameras in McDonalds, at ATM machines, E-Z pass automatically recording the trip through the toll booths, sensors and RFID tags are all aspects of this changing technology. One has just to look at disappearance of pay phones[8] to realize how much the way we communicate, both in frequency and in mode, has substantially changed from only a generation ago.

If Congress were not to preserve law-enforcement's capability to wiretap, what investigative tools might be offered in trade? A clear one is easy access to communications transactional information. One of the non-controversial aspects of the Patriot Act is that it simplified the procedure for obtaining pen register and trap-and-trace orders, no longer requiring an application in each jurisdiction, but letting a single application suffice. Traffic analysis has become significantly easier to obtain and it may be appropriate to trade further capabilities in this direction. For example, the decreasing costs of storage have made record saving much less onerous. Might it be appropriate to require service providers to keep records of communications (which numbers, when, for how long) for a specified

[8] The new wing at Bradley Airport in Hartford, Connecticut, which has twelve gates, has exactly two pay phones.

period in exchange for deciding that communications systems will not be required to be built wiretap accessible?

The threat of terrorism will confront our society for a long time. But we should not necessarily be extending a 1960s wiretap law into the twenty-first century. Instead we should be examining first principles to determine what surveillance laws are appropriate for current challenges. Wiretapping became a law-enforcement tool in the late 1920s; its use was codified in the 1960s and 1970s. If attempting to preserve the tool in order to enable investigators to hold onto this capability would freeze communications in an antiquated technology, that may be the wrong route for our society to take. It may be that few security benefits accrue from the requirement that electronic communications be designed "wiretap accessible" while efforts to do so significantly impede innovation. It is time to fully examine electronic surveillance: it value, needs, and costs. Such a discussion is a necessity in our complicated times. It is crucial as we attempt to solve the current threats to security and liberty.

References

1. Administrative Office of the U.S. Courts, Washington D.C., *1995 Wiretap Report.*
2. Administrative Office of the U.S. Courts, Washington D.C., *2003 Wiretap Report.*
3. Anderson, Betsy and Todd Buchholz, "Memo for Jim Jukes," 22 May 1992 in [16].
4. Brandeis, Louis, Dissenting opinion in *Olmstead v. United States*, 277 U.S. 438, 1928.
5. Brooke, James, "Prosecutors in Bomb Trial Focus on Time Span and Truck Rental," *New York Times,* May 10, 1997, p. A1 and A10.
6. Brooks, John, *Telephone: the First Hundred Years,* Harper and Row, 1975.
7. Duncan Campbell, "Interception 2000: Development of Surveillance Technology and Risk of Abuse of Economic Information," Report to the Director General for Research of the European Parliament, Luxembourg, April 1999.
8. Clark, Ramsey. (1967), in [44, pp. 285-321].
9. Congressional Quarterly Weekly 1968b Congressional Quarterly Weekly, (1968b), Vol. 26, Washington, D.C., July 19.
10. Dam, Kenneth and Herbert Lin (eds.), Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, National Resource Council, *Cryptography's Role in Securing the Information Society,* National Academy Press, 1996.
11. Dempsey, James X., "Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy," *Albany Law Journal of Science and Technology,* Vol. 8, No. 1, 1997.
12. Dempsey, James X. and David Cole, *Terrorism and the Constitution: Sacrificing Civil Liberties in the Name of National Security,* First Amendment Foundation, 1999.
13. Diffie, Whitfield and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption,* MIT Press, 1998.
14. Department of Commerce, Bureau of Export Administration: 15 CFR Parts 734, 740, 742, 770, 772, and 774, Docket No. RIN: 0694-AC11, Revisions to Encryption Items. Effective January 14, 2000.

15. Electronic Frontier Foundation, *Analysis of the FBI Proposal Regarding Digital Telephony,* 17, September 1992.
16. Electronic Privacy Information Center, David Banisar (ed.), *1994 Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal, and Export Controls,* Diane Publishing, Upland, PA., 1994.
17. Electronic Privacy Information Center, *1996 EPIC Cryptography and Privacy Sourcebook: Documents on Wiretapping, Cryptography, the Clipper Chip, Key Escrow and Export Controls*, Diane Publishing Co., Upland, PA, 1996.
18. Federal Bureau of Investigation, "Benefits and Costs of Legislation to Ensure the Government's Continued Capability to Investigate Crime with the Implementation of New Telecommunications Technologies," in [16]
19. Letter to Telecommunications Industry Liaison Unit, Federal Bureau of Investigation, November 13, 1995, in [17, pp. B14-B20].
20. Federal Bureau of Investigation, "Implications of Section 104 of the Communications Act for Law Enforcement," in *Federal Register*, Vol. 62, Number 9, January 14, 1997, pp. 192–1911.
21. Federal Bureau of Investigation, *In the Matter of the United States Department of Justice, the Federal Bureau of Investigation, and the Drug Enforcement Agency: Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act: Joint Petition for Expedited Rulemaking before the Federal Communications Commission,* 10 March 2004.
22. Federal Communications Commission, *Memorandum Opinion and Order,* 10 September 1998.
23. Firestone, David and Dana Canedy, "After the Attacks: The Suspects; FBI Documents Detail the Movements of 19 Men Believed to be Hijackers," *New York Times,* 15 September 2001, p. A1.
24. Freeh, Louis in United States Senate, Committee on the Judiciary, Subcommittee on Technology and the Law (Senate), and United States House of Representatives, Committee on the Judiciary, Subcommittee on Civil and Constitutional Rights, *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services*, Joint Hearings on HR 4922 and S. 2375, March 18 and August 11, 1994, One Hundred Third Congress, Second Session.
25. Hersh, Seymour, "Annals of National Security: What Went Wrong," *The New Yorker*, 8 October 2001.
26. Joint Statement of Industry and Public Interest, *In the Matter of Joint Petition for Rulemaking to Resolve Various Outstanding Issues Concerning the Implementation of the Communications Assistance for Law Enforcement Act,* 27 April 2004.
27. Leone, Richard C. and Greg Anrig Jr. (eds.), *The War on our Freedoms: Civil Liberties in an Age of Terrorism,* Century Foundation, 2002.
28. Levy, Ron, "Memo for Doug Steiner," 26 May 1992, in [16].
29. Lewis, Anthony, "Robert Kennedy Vows in Georgia to Act on Rights, *New York Times*, May 7, 1961, p. 1.
30. Markoff, John, "Cellular Industry Rejects U.S. Plan for Surveillance," *New York Times*, September 20, 1996, p. A1.
31. McIntosh, David and James Gattuso, "Memo for Jim Jukes," 22 May 1992, in [16].
32. Neilsen/Net Ratings, "Broadband Growth Trend."
33. The President's Commission on Law Enforcement and the Administration of Justice, *The Challenge of Crime in a Free Society*, United States Government Printing

Office, 1967.
34. Odlyzko, Andrew, "Content is not King," http://www.dtc.umn.edu//*sim*odlyzko/doc/networks.html
35. *NWG, RFC2804 — IETF Policy on Wiretapping,* May 2000.
36. Risen, James, David Johnston, and Neil A. Lewis, "Harsh CIA Methods Cited in Top Qaeda Interrogations," New York Times, 13 May 2004, p. A1.
37. Rosen, Jeffrey, *The Naked Crowd,* Random House, 2004.
38. Sessions, William, Testimony in [43].
39. Stern, Jessica, *Terror in the Name of God,* Harper Collins Publishers, 2003.
40. Technology and Privacy Advisory Committee, Department of Defense, *Safeguarding Privacy in the Fight Against Terrorism,* March 2004.
41. United States Commission on National Security/Twenty-First Century, *Road Map for National Security: Imperative for Change: Phase III Report of the U.S. Commission on National Security/Twenty-First Century,* 31 January 2001.
42. United States, Senate Select Committee to Study Governmental Operations with respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans, Final Report, Book II*, Report 94-755, Ninety-fourth Congress, Second Session, April 23, 1976.
43. United States Senate, Select Committee on Intelligence, *Senate Select Committe on Intelligence: Inquiry into the FBI Investigation of the Committee in Solidarity wih the People of El Salvador,* Hearings on February 23, April 13, September 14 and 29, 1988, One Hundredth Congress, Second Session.
44. United States House of Representatives, Committee on the Judiciary, Subcommittee No. 5, *Anti-Crime Program*, Hearings on HR 5037, 5038, 5384, 5385 and 5386, March 15, 16, 22, 23, April 5, 7, 10, 12, 19, 20, 26 and 27, 1967, Ninetieth Congress, First Session, 1967.
45. Van Natta Jr., Don and Desmond Butler, "How Tiny Swiss Cellphone Chips Helped Track Global Terror Web," *New York Times,* 4 March 2004, p. A1.