11
Après le Déluge

NSA in 2000

For NSA, the third millennium began in a confrontation with reality. After years of insularity, secrecy, and success with the same old methods, passive interception and an intense focus on cryptanalysis, they had run into difficulty, not with improved cryptography but with the complexity of modern communication (Hersh 1999). It is always difficult to judge intelligence agencies' claims about their problems. It is hardly in their interest to be saying "We are listening to your every word and you had better improve your security." Better to say, "You don't need to do anything special about security. The complexity of modern communication is so great that we can't find the traffic we want to read, let alone decipher it." Nonetheless, for reasons outlined in previous chapters NSA's story has a ring of some truth. Communications had changed dramatically in a very few years and it was not clear that NSA was putting its efforts into the right endeavors.

The agency's director, General Michael Hayden, set out to solve the problem with a change in style, placing a variety of outsiders in critical positions and, like businesses all over the world, outsourcing as much of its activity as possible in an attempt to gain efficiency and save money.

The agency gave its modernization projects heroic names like Trailblazer and Groundbreaker. Reports suggest that these have been less than entirely successful but, as with the initial reports of difficulty, such information is hard to judge. What seems likely is that some people and groups at the agency have a good understanding of the modern world

of communications and are at the cutting edge of intercept technology and practice. NSA, however, is an organization with tens of thousands of employees and decades of established practice. Bringing the entire organization "up to speed" with its best pieces is a difficult task.

Censorship and Surveillance

Automation has allowed many organizations less well known and less formidable than NSA or other national SIGINT agencies to conduct surveillance and outright censorship on traffic.

Employer Web usage policies policed by firewalls

The police and intelligence agencies are supposed to tap your telephone calls only with a warrant. In many circumstances, however, you may be held to have given someone—typically your employer—blanket permission to listen to your communications. The federal government is allowed to monitor the communications into and out of its sensitive agencies to be sure that employees are not talking about classified subjects on unsecured lines. Commercial employees who deal with the public are generally subject to having their calls recorded for "quality-control purposes." To listen to the call that private-sector employees make from their desks at work, however, employers generally need a reason.

The same cannot be said of more modern forms of communication; email and Web browsing, which can be freely intercepted, inspected, and censored in the ordinary course of doing business. The justification offered has some appeal. Indiscreet telephone conversations can reveal critical tidbits but cannot convey programs or large org charts or chip masks. It is hard not to see some legitimacy in an employer's desire to insure that channels that are capable of carrying such information are only used for legitimate purposes. Employees may be unhappy if their employers treat them like children by limiting their web browsing but they are pleased when similar measures prevent their computers from being infected with viruses. Large organizations typically scan incoming mail for viruses and some also scan outgoing mail. In a sense, this is censorship but it certainly makes the online world more livable.

Cryptologie Après le Déluge

As is painfully well known, the terrorist attacks of 9/11/2001 reinvigorated the security and intelligence services of the whole world, and those of the United States in particular. Curiously, they had no immediate effect on the course of US cryptographic policy.

Adoption of AES and CNSS15

Proponents of cryptography worried that the government would renew its attack on the field by claiming that it did not detect the hijacker's plot because it had not been able to read the terrorists' encrypted messages. Instead the response was surprisingly muted. On September 14, Senator Judd Gregg proposed a ban on "unbreakable" cryptography (McAuliffe). His proposal, however, found little support and was withdrawn in mid October (McCullagh 2001b).

That the attacks might delay or derail final approval of the new Advanced Encryption Standard—whose adoption had informally been announced for September—still seemed possible. On November 26, 2001, however, the Secretary of Commerce signed and AES was adopted as Federal Information Processing Standard 197.

The Pentagon's approval of AES for protection of national security systems and NSA development of Suite B, both described in the last chapter, followed. In the US, the struggle over privacy of communications versus surveillance was moving in a new direction.

Things were not quite the same in Britain, which was adopting a course intermediate between the old US policy of discouraging the free use of cryptography and the current one of promoting it. As its name suggests, the Regulation of Investigatory Powers Act[1] expands the snooping powers of British police and intelligence organizations. One of the more controversial provisions of RIPA is a requirement that users must disclose the keys to encrypted data in response to investigators' demands. Although RIPA was passed in 2000, implementation of regulations requiring key disclosure did not begin until 2006. At the time of writing the consultation process has not been completed and no regulations have been implemented. There is therefore no experience with how such regulations work, whether it would be feasible to refute claims of forgotten keys,

how the law would apply to ephemeral keying, etc. It is equally unclear how the legal concept of key disclosure, even if it is successful in Britain, would fare under US law.

Expansion of Intelligence

After 9/11, as after Pearl Harbor, there was a universal feeling of "How could be have been caught by surprise this way?" The fall guy was the intelligence community. Why hadn't they detected the plot? The obvious question "Why should you expect to be able to detect every activity involving two dozen people and half a million dollars over two years?" was obscured by the fact that we seem almost to have discovered the plot in several places. If only intelligence and law enforcement had been more vigilant, perhaps the attacks could have been prevented.

The country's response was to retarget intelligence—which for decades had been shaped by the objective of watching the Soviet Union and its allies—toward attempting to watch the far more elusive target of "worldwide terrorism." In particular, signals intelligence expanded and shifted its focus: less effort listening to dedicated military communications; more effort intercepting commercial channels accessible to small less-well-funded organizations.

FISA taps, the foreign intelligence taps named after the legislation that authorized their use,[2] became a subject of public interest after the attack. How had the United States missed the plot? What had prevented the CIA from telling the FBI about Khaled al-Mihdhar and Nawaf al-Hazmi,[3] who were in the United States in the months before September 11, 2001? (They clearly weren't here to "visit Disneyland" (Wright 2006, p. 354).) Why hadn't the US government uncovered the plotters' plans? Should there be changes to wiretap law? In the aftermath of 9/11, the Department of Justice made a number of legislative proposals; an important one concerned the relationship between FISA and Title III wiretaps. Instead of foreign intelligence being the *primary* reason for a FISA wiretap, the USA PATRIOT Act,[4] the law hurriedly enacted after the 9/11 attacks—and which will be discussed in some detail shortly—modified FISA taps so that foreign intelligence had only to be a *significant* reason[5] for the taps.

The change was only a single word, but it was a very important single

word. In issuing a wiretap warrant for a criminal investigation, the 1968 law, sometimes referred to as "Title III," requires probable cause that the individual named in the order is committing or is about to commit an indictable offense. FISA is much less stringent, stating simply that there is probable cause to believe the individual is an agent of a foreign power. Wiretapping, in which no notice is given until after the tapping is over (in the case of FISA, notice may never be given) and which may go on for months, is particularly insidious, and the less exacting requirements for FISA—establishing that the suspect is an agent of a foreign power rather than someone committing or about to commit an indictable offense—was deemed appropriate because foreign intelligence warrants are for information collection, not for criminal prosecution.

There was an escape clause: if during a foreign intelligence investigation, facts emerged indicating a federal crime had been, or was about to be committed, intelligence officers were to inform criminal investigators, who would begin an investigation. Such a policy had existed through several presidential administrations, and the policy was explicitly laid out in a memo from President Clinton's Attorney General, Janet Reno, a memo that was later endorsed by the incoming Bush administration in 2001 (Thompson 2001). The policy had explicit procedures for informing the FBI Criminal Division if a FISA investigation exhibited criminal aspects; it also made clear that the criminal division was not to "run" the FISA investigation (Reno 1995). Then 9/11 occurred and, with it, the Moussaoui case.[6] In such situations, it is often easier to act than to analyze. The change in FISA—along with the rest of the USA PATRIOT Act—was proposed and enacted within six weeks of the 9/11 attacks.

It was difficult to know if the modification was actually needed. In contrast with Title III wiretaps, of which there is a public account,[7] only the number of FISA orders (furnished annually to Congress) is disclosed, except in the rare case when the information gathered from FISA surveillance is used in a public trial.

In 2002, the Attorney General proposed a new set of procedures for FISA cases that would simplify the issue of the walls. The FISA Court was not pleased with these. Earlier the Justice Department had informed the court of mistakes in FISA applications. The court's opinion took these problems into account and was quite critical of the proposal (USFISC

2002a). Senate Judiciary Committee members Leahy, Specter, and Grassley requested that the FISA Court provide the Senate oversight committees with copies of this opinion; not only did the FISA Court decide to do so, but it went one step further and made the opinion public as well (Kollar-Kotelly 2002).

The FISA Court criticized FBI mishandling of the wall in foreign intelligence cases and criminal investigations:

- Information on FISA investigations had been shared with criminal investigators in the New York FBI field office without consultation of the FISA Court, as was required. (USFISC 2002a, p. 17)
- More than 75 FISA applications related to major terrorist attacks directed against the United States had misstatements or omissions of material facts including: an erroneous statement that a FISA target was not under criminal investigation; false statements concealing overlapping intelligence and criminal investigations, and unauthorized sharing of FISA information with FBI criminal investigators and assistant US attorneys; omission in FBI affidavits of a previous relationship between the FBI and a FISA target. (USFISC 2002a, p. 17)
- In another FISA case, where there was supposed to be a wall between the intelligence and criminal investigations, there was no separation. Instead the case was run by a single FBI squad and all screening was done by a single supervisor overseeing both investigations. (ibid., p. 17)

The Court went on to say that "in virtually every instance, the government's misstatements and omissions in FISA applications and violations of the Court's orders involved information sharing and unauthorized disseminations to criminal investigators and prosecutors. These incidents have been under investigation by the FBI's and the Justice Department's Offices of Professional Responsibility for more than one year to determine how the violations occurred in the field offices, and how the misinformation found its way into the FISA applications and remained uncorrected for more than one year despite procedures to verify the accuracy of FISA pleadings." (ibid., p. 18)

The FISA Court announced that it would no longer accept inaccurate FBI affidavits regardless of what caused the inaccuracy (ibid., p. 17). It barred an unnamed FBI agent from signing affidavits for the FISA Court (ibid., p. 17). And, for the period from March 2000, when the problem first came to light, until September 15, 2001, the court—in a manner more reminiscent of scolding an errant child than instructing federal prosecutors—required all Department of Justice personnel receiving certain FISA information to certify that they understood the wall procedures used to separate FISA investigations from criminal prosecutions (ibid., p. 18). Stewart Baker, former chief counsel of NSA and a man who might be expected to be on the side of federal investigators, deemed the FISA Court report a "a public rebuke" (Eggen and Schmidt 2002).

There was more. With respect to one particular FISA application, the court approved the wiretap order but ordered that

> law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division [of the Department of Justice] shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives. (USFISC 2002b, p. 3)[8]

In order to handle the issue of the wall, the FISA Court used a chaperone as the protector of liberty: the Office of Intelligence Policy and Review. OIPR, an office of the Department of Justice responsible for advising the Attorney General on intelligence matters, was to 'be invited' to meetings between the FBI and the Criminal Division to prevent any further diversion of FISA searches and surveillances towards law enforcement objectives (ibid., pp. 12–13).

For the first time since the 1978 enactment of FISA, the US government appealed a FISA Court decision. The United States Foreign Intelligence Surveillance Court of Review convened, and decided in favor of the administration: the FISA Court had "misinterpreted and misapplied minimization procedures it was entitled to impose" (USFISCR) and had not properly interpreted the PATRIOT Act's change to FISA. The Review Court concluded that the government is not obligated to prove to the

FISA Court that the primary purpose in conducting electronic surveillance in a particular investigation is not criminal prosecution (USFISCR). The Review Court examined the reasonableness of FISA searches under the Fourth Amendment; it did not explicitly rule on the issue, but it did state "we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close."

Despite the Court of Review's failure to back the lower court's actions, there were other voices saying that bringing down the wall had gone too far. As Senators Leahy, Grassley, and Specter reported, in regard to FISA implementation failures (Leahy et al. 2003), there were a surprising number of serious problems: FBI headquarters did not properly support the FBI field offices in foreign intelligence issues and key agents were inadequately trained both in FISA *and* in aspects of criminal law. While secrecy about actual FISA cases is appropriate, secrecy within the FBI about FISA policies and procedures is not. As a result, the Bureau was hamstrung; the FBI's inability to analyze and disseminate intelligence information—"[T]he FBI did not know what it knew"—undermined the bureau's ability to do its job. The report also observed that these breakdowns resulted in a mishandling of the Moussaoui FISA application (ibid.). It looked as if the FBI, rather than the wall, was the real barrier hampering investigations.

The number of FISA taps continues to rise. From an average of about 500 in the 1990s, after 2001, the number of FISA wiretaps steadily increased. In the most-recently-reported year, 2005, there were 2072 FISA applications, all of which were approved by the FISA Court (which did make "substantive modifications" to 61 of these (Moschella 2006). The number of emergency FISA orders, which allow surveillance to be initiated *before* a court order has been approved and give the government seventy-two hours thereafter to obtain the order, was also substantially higher. Attorney General John Ashcroft testified that in 2002 he had signed 170 emergency FISA warrants. That number was more than three times the number of emergency FISA orders issued in the preceding 23 years (Ashcroft 2003).

The senators who had agreed to the PATRIOT Act change to FISA did not approve of the way this change had manifested itself. In hearings

in 2002, Judiciary Committee Chairman Senator Leahy reminded the administration that "it was not the intent of [PATRIOT Act] amendments to fundamentally change FISA from a foreign intelligence tool into a criminal law enforcement tool." (USSH 107 *USA PATRIOT ACT in Practice*, p. 4) Senator Arlen Specter, the ranking Republican of the Judiciary Committee, complained: "When the purpose of the FISA Act was foreign intelligence and the court interpreted 'purpose' as 'primary purpose,' the change was made to 'significant purpose.' But then the Department of Justice came in with its regulation and said that since the PATRIOT Act said a significant purpose was foreign intelligence, then the primary purpose must be law enforcement—which is just, simply stated, ridiculous. The word 'significant' was added to make it a little easier for law enforcement to have access to FISA material, but not to make law enforcement the primary purpose." (ibid., p. 33) Leahy warned: "The Department is urging broader use of the FISA in criminal cases. And you are going to lose, ultimately lose public confidence both in the Department and in the courts, unless you can, by public reporting or otherwise show this is being used appropriately." (ibid., p. 37)

The USA PATRIOT Act

The Title III wiretap law was several years in the making and evolved through various studies and countless hearings. By contrast, the Anti-Terrorism Act of 2001, almost all of which became the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001—the USA PATRIOT Act—was brought to Congress on September 19, 2001, just eight days after the terrorist attacks of 9/11 (O'Harrow 2005, p. 23). The PATRIOT Act was wideranging and represented a "shopping list" for the Department of Justice. As later studies showed, it was not the lack of tools that prevented US intelligence from finding the hijackers before September 11, but rather a problem of coordination between agencies (and within agencies). But in the fall of 2001 the atmosphere in the United States was tense and highly fearful and despite strong efforts by civil libertarians, the PATRIOT Act did not receive much public scrutiny. The act passed a little less than five weeks later, in the midst of the anthrax attacks.[9] In

discussing the PATRIOT Act, our focus will be on those sections of the law related to wiretapping and electronic surveillance.

From a wiretapping perspective, the most significant aspect of the PATRIOT Act was the change we have already examined, namely the §220 shift in purpose in FISA wiretaps from foreign intelligence necessarily being a "primary" reason of the wiretap order to merely being a "significant" reason.[10] The PATRIOT Act wiretapping and electronic surveillance provisions include:

- Expansion of Title III list of serious crimes predicating a wiretap investigation:

  §201 added terrorism and production or dissemination of chemical weapons to the list of serious crimes under Title III. Since it was already possible to obtain a FISA warrant to investigate these crimes, the purpose of §201 was to extend the capability of investigating a US person suspected of domestic terrorism activities.

  §202 added "felony violation of section 1030 (relating to computer fraud and abuse)" to the list of serious crimes under Title III.[11]

- Ability of law enforcement to share electronic surveillance information with national-security officials:

  §203(b) permitted law-enforcement officials to share information obtained from a wiretap or other forms of electronic surveillance with "any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official."

- Emergency disclosure of electronic communications:

  §212 allowed ISPs to voluntarily release subscriber content and records to the government if there is reason to believe that there is an immediate danger of death or serious injury.

- Changes in laws governing pen register and trap-and-trace devices:

  §214 removed the requirement under FISA that the government prove the target is "an agent of a foreign power" before the court would approve the installation of a pen register or trap-and-trace device. This section included a provision prohibiting use of FISA

pen register surveillance against a United States citizen where the investigation is conducted solely on the basis of protected First Amendment activities.

§216 modified the definition of these tools to make it clear that they applied to the Internet; amended the definition of the tools to include a prohibition on content collection; required that records of pen register and trap-and-trace devices must be provided under seal to the court within thirty days of installation.

- Single Application for Nationwide Wiretap and Surveillance Orders

  §220 expanded the authority of a court-authorized wiretap order or pen register/trap-and-trace device order to apply nationally. Previously the orders had held only in the jurisdiction of the court, thus forcing law enforcement to apply in multiple jurisdictions for what was essentially a single wiretap or pen register/trap-and-trace device order.

- Roving Wiretaps:

  §206 expanded FISA authority to include roving wiretaps (previously only Title III wiretaps could be roving).

- Other Issues:

  §207 extended the duration of a FISA wiretap for non US persons who were agents of a foreign power to ninety days unless otherwise specified.

  §210 expanded law enforcement's ability to gather information through subpoena. Previously law enforcement could obtain the "name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service or a subscriber to or customer of such service and the type of services the subscriber or customer utilized" from an ISP. §210 requires the service provider to disclose records of session times and duration; any temporarily assigned network address; and any means or source of payment.

§211 amended Title III to apply to cable operators providing telephone and Internet services.

§217 permitted warrantless government interception of the communications of a computer trespasser if the owner or operator of a "protected" computer authorizes the interception. "Protected" computers include any "used in interstate or foreign commerce or communication."

§223 permitted individuals to sue the government for unauthorized disclosure of surveillance information.

§225 eliminated civil liability for a carrier complying with a FISA wiretap or emergency order.

Certain clauses were due to "sunset" in 2005 unless explicitly extended by Congress. These included: §201 on adding terrorism to the list of serious crimes warranting a Title III wiretap search; §202 on similarly adding computer fraud to that list; §203 (b), on sharing criminal wiretap information with intelligence agencies; §206 FISA roving wiretaps; §207 extended the duration of FISA taps for non-US persons; §214 lowered standards for FISA pen registers and trap-and-trace devices; §217 warrantless interception of the communications of a computer trespasser; §218 the "significant purpose" provision, and §220 nationwide authorization for search warrants for electronic evidence. In the fall of 2005, because of civil-liberties concerns there was much dispute about extending these provisions and the PATRIOT Act was only temporarily extended.[12]

In the end, all the provisions were extended with modifications made to §206. The changes to §206 included a requirement that the wiretap order describe the *specific* target of the surveillance if the target's identity is not known,[13] that the FISA court must determine that the roving wiretap is needed based on specific facts about the target included in the application for the wiretap, and that whenever a new location is tapped under the order, the government must notify the FISA court within ten days[14] of[15] (i) the location of each new facility at which the surveillance is taking place, (ii) why these location changes occurred, (iii) a description of the minimization procedures being used if the minimization procedures are

different from those in the original order, and (iv) the total number of surveillances being conducted (Yeh and Doyle 2006, pp. 17–18).

One noteworthy feature of the PATRIOT Act strikes at legal doctrines far older than electronic surveillance. The US took from British law the notion of *knock and announce*: police searching premises would at least attempt to inform the occupants at the time the warrant was being executed. The doctrine was gradually eroded by court tolerance of the need to make secret entries to install bugs. In the investigation of the spy Aldrich Ames Ames, however, the FISA court went a step farther and authorized a secret search. This might have derailed the Ames case, but Ames was persuaded to plead guilty by promises that if he did his wife would be treated more leniently. Because the Constitution does not address the issue of whether police must announce themselves for a search to be reasonable, this appears to be a matter of law rather than a constitutional issue. In 1994 FISA was amended to allow such "sneak and peek" searches in intelligence investigations, including cases of international terrorism (before that, the Attorney General had authorized such searches without judicial oversight). Section 213 of the PATRIOT Act authorizes the use of these delayed-notice searches, in which the target is told of the search but *after* (possibly quite some time after) the search has occurred, for any case in which providing notice might have an adverse effect on an investigation or unduly delay a trial. The Department of Justice has said that such searches have occurred in non-terrorism cases.

NIST's Computer Security Division

GISRA and FISMA

The White House Office of Management and Budget, which had been disturbed about the poor state of computer security in federal civilian agencies, thought the Congressional attention focused on Y2K[16] and encryption policy might lead to willingness for further action, such as on computer security in federal civilian agencies. This was the genesis of the Government Information Security Reform Act (GISRA),[17] which required agencies to do internal risk assessments and submit those results to the Office of Management and Budget, which followed up with reports to Congress.

GISRA applied for only a year; its provisions were reauthorized and strengthened by Title III of the E-Government Act of 2002,[18] the Federal Information Security Management Act (FISMA).[19]

FISMA included an enforcement provision; agency budgets were in danger if the agency did not comply with FISMA. Congress strengthened enforcement in another way. The Computer Security Act of 1987 permitted agencies to obtain waivers from NIST's cybersecurity recommendations; under FISMA, the Secretary of Commerce had authority to make NIST information system standards and guidelines mandatory. NIST's Computer Security Division now had an enforceable role in securing the government's non national-security systems.

CSD Stays at NIST

In January 2000 the White House announced the change in encryption export controls, and despite Senator Gregg's call, in the wake of 9/11, for encryption controls, the government's policy did not waver. Then an odd thing happened. In the summer of 2002, the White House announced its support for the creation of the Department of Homeland Security, a consolidation it had previously opposed. When the draft bill surfaced, all the usual suspects—the Coast Guard, the Federal Emergency Management Agency, the Transportation Security Administration—were in the new department. There was also a surprise: NIST's Computer Security Division, the group that provided cryptographic standards[20]

for US government civilian agencies, was also slated to be moved.

The rationale for the proposed move was that since protecting critical infrastructure properly belonged in the new department, so did the Computer Security Division (CSD). US industry did not like the idea. With the CSD part of the Department of Commerce, business and industry had input into the CSD standards development process. Indeed, the Advanced Encryption Standard development was a clear demonstration of how well government and industry were working together, to everyone's benefit. Moving CSD to Homeland Security would place the division in a department more focused with law-enforcement concerns than on commerce, and would likely reignite the crypto wars—or worse. There was opposition from industry and civil-liberties groups to the proposed

move, and NIST's Computer Security Division ended up staying right where it had been. Standards for protecting critical infrastructure would be developed in the Department of Homeland Security, with help and coordination from CSD, as needed.

Funding, however, was a concern. CSD had been chronically underfunded from the beginning. One bright spot of the proposed move had been the potential for appropriate levels of funding. Various groups, from industry lobbyists to the Information Security and Privacy Advisory Board, a federal advisory committee, swung into action. They lobbied Congress, describing the broad value of the Computer Security Division's work to the federal government *and* to US industry,[21] and they cited the increased role of the Computer Security Division under FISMA. At a time when science agencies saw level or even reduced funding, the Computer Security Division's support doubled (from approximately $10 million to $20 million),[22] a more reasonable sum—though still small—given the enormity of the job.

Data Retention and Data Mining

In 1900 there were some 1.5 billion people in the world and no database of 1.5 billion items. A century later, there are 6 billion people, and a 60-gigabyte disk—a disk roughly big enough to store everyone's name—costs less than $100. Ten times that much storage—enough to store everyone's name and address and maybe a bit more—costs about $500. Within a few years, the storage needed to store a short biography (or dossier, if you prefer) of every person on Earth will be within the reach of many of those people.

There is probably as yet no list of everyone's name let alone a single collection containing everyone's biography but the implications for privacy are clear. The most obvious barrier to keeping records on everyone—the inability to manage the database—is falling, thereby preparing the way for compiling such a database.

The falling cost of storage has other implications. For over a decade now, video cameras have been proliferating in and beyond the industrialized world. Because videotape is cheap, there is no need to reuse; many of these cameras are always recording new tape and contributing

to an ever-growing archive. Other sources of raw data are recordings of intercepted signals, billing records for communications and many other kinds of transactions, including such information as the movements of drivers who pay their tolls with "EZPass" devices.[23]

The information in these various existing repositories is not always very useful. The databases themselves are scattered and the information they contain is not always readily linked to human identities. Bit by bit, however, the technology to extract useful information form a welter of low-grade information is being developed and the extraction of information is following a path similar to that of gold, oil, and other valuable minerals. At one time only the richest gold mines and the richest oil fields were worth developing. As time passed, gold and oil grew more expensive and the means to extract them grew cheaper, so the gold diggers and oil drillers began to go after lower grade ore.

The analogy is lost on no one and the technology for extracting valuable information from low-value inputs is called *datamining*. The subject presents many difficult problems, most notably transcribing speech and recognizing people, but it is making rapid progress.

For information to be processed, of course, it must be available to the people who have the means and the desire to process it. Often valuable information is collected and soon disposed of either because it is no longer needed or as an explicit privacy protection measure. National police and intelligence organizations have sought to counter this problem by pushing for laws requiring *data retention*, the intentional storage of data beyond the time it would be needed for the purpose for which it was originally collected. The explicit intent of such laws is to make the information available for criminal investigations that might take years to develop but it also has another effect. The longer data are retained—particularly when they are retained under threat of serious penalties for their loss—the more likely they are to proliferate and to live beyond their intended lifetime.

The events of 9/11 derailed various efforts heading for increased citizen privacy and even turned some completely around. One such, previously described, was Carnivore. Another was data retention, the issue of to what extent communications carriers should routinely archive informa-

tion about users' telephone calls, emails, and other communications. In this case, the first action was in Europe—or so it appeared.

In 2000 the European Commission issued a draft privacy proposal that included new protections for electronic communications. The European Council of Ministers, the EU's main decision-making body, did not oppose the effort but sought to include data-retention requirements in the proposal. In July 2001, the European Parliament's Civil Liberties Committee approved a draft directive stating support of "strict regulation of law enforcement authorities' access to personal data of citizens, such as communication traffic" (Lynch 2001). Then 9/11 occurred, and the UK and Dutch Members of the European Parliament strongly opposed the rules that had been drafted by the Civil Liberties Committee. So did someone else. In a letter from James Foster, deputy chief of the US mission to the European Union, the White House requested that the directive "permit the retention of critical data for a reasonable period" (Meller 2001). The United States had no such requirements.

Changes ensued in the European directive. Pressure from two Spanish MEPs and the European Council resulted in passage of a directive somewhat different from the original: "Member States, may ... adopt legislative measures providing for the retention of data for a limited period justified on the grounds [to justify national security (i.e., State security), defence, public security, and the prevention, investigation, and detection of criminal offences]" (European Union 2002, p. 34).

Implementation remained elusive, however. In the E.U., harmonization of such directives across the member states is critical, but in this case, the member states held sharply differing views on the privacy protections needed. Here is where European and American viewpoints sharply differ. European law requires *proportionality:* "proportionality of the measure in relation to costs, privacy (data protection), and efficacy" (Council of European Union 2005, p. 1). Thus a proposal for three-year data retention made by Denmark, Ireland, Sweden, and the United Kingdom was rejected (European Parliament 2005). The issue went back and forth and finally, in December 2005, the European Parliament passed a directive requiring telephone companies and ISPs to retain traffic data on *all* messages and phone calls for between 6 and 24 months (Best 2005). Data

was to be kept *even* on unanswered calls. With this directive in place, member states were now free to implement the directive.

So were some non-member states. There had been public silence on this issue in the United States. But after the passage of the European directive, in the spring of 2006, Attorney General Alberto Gonzalez called on Congress to pass data-retention laws to combat child pornography. Several bills are in preparation.

CALEA Revisited

By 2003 the main issues, at least on the legal front, in applying CALEA to digital telephony had been resolved and the FBI turned its attention to a new issue: wiretapping VoIP (Bellovin 2006a). In a letter to the FCC in November 2003, the FBI gave notice about its growing concern (Milonovich 2003). Four months later the FBI submitted a formal petition asking the commission to clarify which VoIP services were subject to CALEA (FBI 2003). There was surprise in some circles: after all, during his 1994 testimony, FBI Director Freeh had made clear that the proposed law was limited to the telephone network.[24] As a result of complex negotiations, CALEA explicitly stated:

> (8) The term 'telecommunications carrier'—
>
> (C) does not include—
>
> (i) persons or entities insofar as they are engaged in providing information services; and
>
> (ii) any class or category of telecommunications carriers that the Commission exempts by rule after consultation with the Attorney General.[25]

and that the capability requirements for wiretapping did not apply to information services.[26]

CALEA applied to VoIP presents a number of complexities, complexities to which it appeared the FBI paid little attention. The real issue was not about wiretapping *per se*—there was no disagreement about the applicability of wiretap law to Internet communications—but about applying CALEA, and FBI design standards, to the Internet. The Public Switched Telephone Network and the Internet are two distinct communication networks. They may rely upon the same underlying transmission

facilities and even share the same cables; both may use electronic routing and switching devices at central nodes to move bits efficiently through the network from one user to another; and both may use digital transmission and some form of time-division multiplexing (Bellovin 2006a, p. 9). But circuit-switched networks and packet-routed networks are very different and no amount of calling both "communications networks" can obliterate the differences: techniques that work for wiretapping in one are, in many cases, simply not feasible in the other. Although opponents of the FBI request believed that CALEA's lack of applicability to Internet applications was clear, not everyone agreed.

The FCC, in particular, sided with the FBI. In the summer of 2005, it announced that CALEA applied to two types of VoIP service: providers offering transmission or switching capabilities *on their own lines* between the end user and the Internet (facilities-based) and providers offering service that enabled the connection between an end user on the telephone network and VoIP.[27] The American Council on Education, whose members were concerned about the cost of applying CALEA to their internal networks, various civil-liberties groups, and the computer and telecommunications industry pressed the FCC for a stay; when that failed, they turned to the courts. In June 2006, somewhat to their surprise,[28] in a two-to-one decision, the US Court of Appeals agreed with the FCC and the FBI *American Council on Education, Petitioner v. Federal Communications Commission and United States of America*, No. 05-1404 et al. (D.C. App. June 9, 2006).[29]

These two particular types of VoIP services have architectures that fundamentally resemble the telephone network and thus their accommodation of CALEA is not particularly difficult.[30] That is not true for other VoIP services. VoIP, like much of Internet communication, is about mobility and mobility does not come for free. In some cases—intercept against a call from a fixed location with a fixed internet address connecting directly to a big Internet provider's access router—VoIP is equivalent to a normal phone call, and the interception does not present a technical challenge (Bellovin 2006a, p. 2). But if *any* of these conditions is not met—if the VoIP call is at all mobile—then the problem of assuring interception becomes enormously harder (ibid).

Before CALEA came into the picture, wiretapping was done some-

where along the *local loop*, the pair of wires running from the local telephone switch to the subscriber's phone. The local-loop wiretap receives all the information that travels down those wires, but it does *not* capture information, such as forwarded calls, that are diverted at the switch and do not travel on the local loop. The FBI sought CALEA to ensure that telephone standards would be designed to eliminate such problems, thus enabling full legally-authorized wiretapping. As discussed in chapter 5, the solution is to make the wiretap a silent participant in a conference call. Then all the information available to the local switch—call-forwarding, speed call lists, caller identities—is also available to the wiretap.

Internet users rarely know the IP addresses of the people with whom they communicate. In the old days computers were fixed and so were their IP addresses. Now a user may connect from an Internet cafe at 10, a conference room at noon, and airport lounge at 3, and each of these will have its own IP address—usually more than one. In the current scheme of things, Internet addresses are, more often than not, allocated dynamically, which means that the address the laptop had on Monday at 10 A.M. at the Cozy Corner Cafe is likely to be different from the one it acquires there on Tuesday. Thus the first step of a VoIP service is to take a familiar identifier—a user name, a telephone number, an email address—and transform it into a specific IP address where the user can currently be found. This is called a *rendezvous* service.

Once the association between name and current IP address has been established, the actual voice call can travel in myriad ways. Consider the VoIP network shown in figure 11.1. Alice and Bob are both currently connected via the ISP C using router R1 and ISP D using router R2, respectively. Alice, however, uses VoIP Provider 1, a customer of ISP A, while Bob gets his service from VoIP Provider 2, a customer of ISP B. Both Alice and Bob are traveling and thus are in varying locations; they connect via different ISPs without changing their VoIP providers.[31]

When Alice calls Bob, her VoIP phone sends a message across the Internet to her VoIP provider, which contacts Bob's VoIP provider, and Bob's VoIP provider in turn notifies Bob. (The flow of the call setup messages is shown via dashed lines.) The actual data flow of the phone conversation can be completely different however; there is *no* requirement that the call

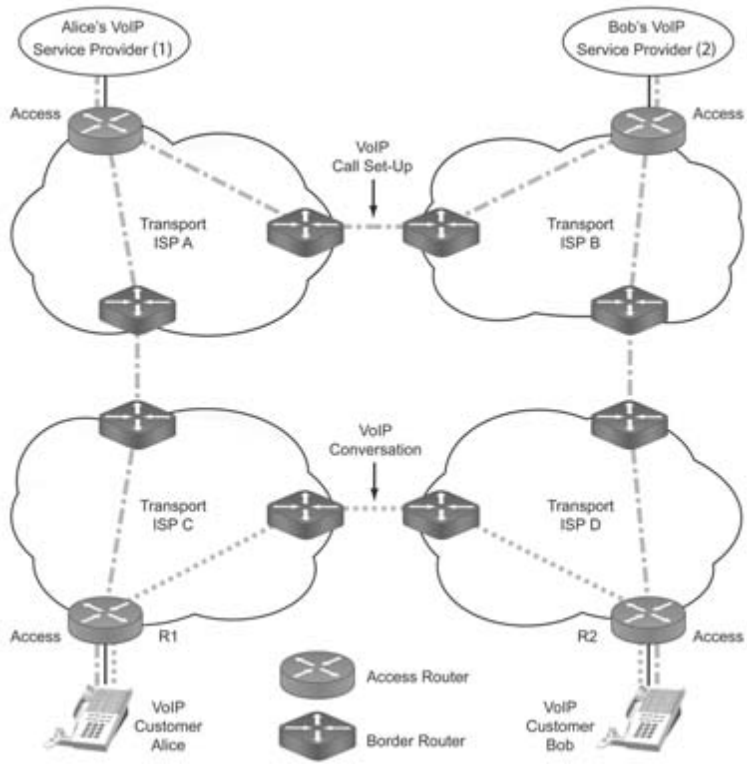


Figure 11.1
Alice and Bob talking via VoIP with multiple providers.
(Illustration by Steve Bellovin and John Treichler.)

go through Alice or Bob's VoIP providers (the call is shown by the two dotted lines).

Suppose we are trying to wiretap Alice's calls to Bob. The obvious points from which to do the tapping are access routers R1 and R2 (these are the Internet analogy—to the extent there is one—of the local telephone switches). However, neither router knows who Alice or Bob are or, for that matter, any information analogous to a telephone number that has a long term connection with Alice or Bob. This is something in the domain of the two VoIP providers. For the tap to succeed, R1 or R2 would have to receive a "start recording" instruction from one of these VoIP providers. But here is where the situation becomes complicated. The VoIP providers can be located at arbitrary places on the Internet,

and they need have no business or technical relationship to any ISP other than their own. In fact, they could easily be located in and owned by foreign (and even hostile) countries. How can Alice's ISP trust such a wiretap request?[32]

If Alice's VoIP Provider is owned by her ISP (that is, ISPs A and C are one and the same), the issue is simpler, and for sure, many broadband ISPs do own VoIP operations. This, however, is not required nor even expected to be the norm. Skype, for example, is a non-US company, and is not associated with any ISP. The disassociation of the VoIP provider from the ISP combined with the mobility of the VoIP user makes CALEA applied to VoIP exceedingly complex. As things stand, investigations targeted against people who are constantly on the move are likely either to fail or to violate the privacy of innocent bystanders.

The old models of communications surveillance do not translate easily to the dynamic, packet-routed, signaling-and-content-combined network architecture that forms the Internet. The Internet's flexibility enables a wide variety of VoIP implementations; some, like those picked off by the current FCC order, simply connect an end user on a telephone to a VoIP network and those can relatively easily accommodate CALEA. Others are genuine peer-to-peer applications. Because of the packet-routing nature of the Internet, the path of a VoIP conversation cannot be predicted—and that seriously complicates the placing of the wiretap. It can't be put on the client device, for danger of being discovered and thwarted. But for the wiretap to be placed anywhere else, there must be some way to determine the route the communication will take, and that is not plausible.

Mobility further exacerbates the wiretapping problem. Not only can't you predict which route an Internet communication will take but because of mobility it is not always simple to tell whose packets are the ones of interest, which presents serious problems for minimization. The ease with which new identities can be created on the Internet, a far simpler process than adding a new phone line, also complicates internet wiretapping.

Finally there is the problem of ensuring safe transport of the wiretap information to the law-enforcement facility, a problem far more complex in the packet-routed world than in its telephone counterpart.

A report examining the FCC order observed:

> Building a comprehensive VoIP intercept capability into the Internet appears to require the cooperation of a very large portion of the routing infrastructure, and the fact that packets are carrying voice is largely irrelevant. Indeed, most of the provisions of the wiretap law do not distinguish among different types of electronic communications. Currently the FBI is focused on applying CALEA's design mandates to VoIP, but there is nothing in wiretapping law that would argue against the extension of intercept design mandates to all types of Internet communications. Indeed, the changes necessary to meet CALEA requirements for VoIP would likely have to be implemented in a way that covered all forms of Internet communication. (Bellovin 2006a, p. 13)

Such modifications to Internet protocols present a clear risk of introducing vulnerabilities into Internet communications. After all, wiretapping is a legally authorized security breach, and introducing a security breach into a communications network always entails serious risks. In 2000 the Network Working Group of the Internet Engineering Task Force (the IETF designs the protocols for the Internet) studied putting wiretap requirements into Internet protocols and concluded that it could not be done securely (IETF 2000). Their conclusion arises from fundamental engineering principles: complexity is the bane of security. Every function added to a secure program must be evaluated to be sure that it does not contain a vulnerability, when used either alone or in combination with other features (Landau 2006, p. 431).

The industry group examining the issue concluded that, "In order to extend authorized interception much beyond the easy scenario, it is necessary either to eliminate the flexibility that Internet communications allow, or else introduce serious security risks to domestic VoIP implementations. The former would have significant negative effects on US ability to innovate, while the latter is simply dangerous. The current FBI and FCC direction on CALEA applied to VoIP carries great risks." (Bellovin 2006b, p. 2)

Of course, VoIP is not society's only form of mobile telephone communication; cellular phones are also mobile. The mobile telephony of cellphones operates very differently from VoIP and makes accommodating wiretapping easier than for VoIP but not as easy as it is on the wireline system. When a cellphone is operating within its home cell, it behaves much like a wireline phone and wiretapping is simply done at the switch. When the cellphone is roaming outside its normal service area, the situation becomes more complex. At the time the roaming

phone is initially turned on, and maybe every fifteen minutes after that, it sends a signaling message back to its home switch.[33] At this point only signaling information has been transferred to the home network. If the roaming cellphone is called, the incoming call passes through its home system during call setup and wiretapping will be initiated at this point. The situation is entirely different, however, when the roaming cellphone makes the call. Once the phone is *registered* with the local switch, if a call is made locally by the cell phone, there is *no* immediate notification about that call to the home switch (or the billing system) and the call is *not* routed through the home switch unless that happens to be the call's destination. This means that no wiretapping can be done on the incoming calls of roaming cellphones by their home switches. It would be possible to route calls artificially back through the target's home system and back again to facilitate wiretapping, but such routing might well be detected by the target due to changes in timing, voice quality, or billing.

There is also the issue of *roving wiretaps*: wiretaps in which, because law enforcement has reason to believe the suspect is using a variety of phones—either because the suspect is trying to avoid a wiretap or because her business is such that she naturally moves around—the telephone number to be tapped is left unspecified in the court order (Solove, pp. 325–326). Law enforcement can, with a single warrant, tap the suspect at Joe's Pizza at 10 and at the bank of phones by Gate 9 East in Penn Station at noon. Roving wiretaps thus appear to mimic VoIP taps. However, minimization, which requires that it is the suspect's call—*and only the suspect's call*—is wiretapped, plays a significant role in distinguishing the two situations. Even if the suspect frequents Joe's Pizza and the bank of telephones at Penn Station, law enforcement cannot have active wiretaps on all the phones at Joe's Pizza or all the telephones by Gate 9 East; rather the wiretap can only be activated when law enforcement knows the suspect is on a particular line. Thus physical surveillance plays a role in roving wiretaps for which there is no analogy in VoIP wiretapping.

The Appeals Court was asked to reconsider its decision in an *en banc* review,[34] but declined. Meanwhile, in a little-noticed policy statement issued the same day as the FCC statement on CALEA applicability, the FCC also announced:

> The Federal Communications Commission today adopted a policy statement that outlines four principles to encourage broadband deployment and pre-

> serve and promote the open and interconnected nature of the public Internet: (1) consumers are entitled to access the lawful Internet content of their choice; (2) consumers are entitled to run applications and services of their choice, subject to the needs of law enforcement; (3) consumers are entitled to connect their choice of legal devices that do not harm the network; and (4) consumers are entitled to competition among network providers, application and service providers, and content providers. Although the Commission did not adopt rules in this regard, it will incorporate these principles into its ongoing policymaking activities. All of these principles are subject to reasonable network management. (FCC 2005b)

The meaning of this statement is not clear; indeed, it seems contradictory. "Encouraging broadband deployment" and "promoting an open and interconnected Internet," seem at odds with being able to "run applications and services of their choice," only "subject to the needs of law enforcement." These needs have not been defined, let alone legislated and the statement was, to many, a threatening stake in the ground. At the time of this writing, a year later, there has been no clarification of the policy statement.

The National Security Agency

Current NSA programs

The basic architecture of US surveillance law from the end of the 1970s on had been simple. Interception of communications outside the United States was governed by policies set by the executive branch, largely by the National Security Agency. These policies were subject to high-level review by the intelligence oversight committees of Congress and rarely came to the attention of the courts. Communications interception inside the United States was governed by either the Title III provisions for wiretaps in ordinary criminal cases or by the Foreign Intelligence Surveillance Act. In either case, warrants, specifying individual targets, were required either before or shortly after the start of interception.

After 9/11, NSA, presumably on the urging or outright orders of the White House, began to relax (or bend, depending on your viewpoint) its rules about communications that were in whole or in part US communications. The issues in question concern both communications that originate or terminate (or both) inside the US and communications to which some of the parties are *US persons* wherever they may be located.

It can be argued that the most dangerous of our terrorist enemies are not those abroad but those who have already entered the United States. These people, however, are part of foreign organizations and can thus be expected to "call home" from time to time. On this logic, a communication with one terminal in the US and the other at a known terrorist location outside would seem to be fair game.

The issues are: Who is the target (outside the US)? Where is the target? How is the traffic being collected? Where is it being collected? The Bush administration believed that FISA did not cover all the legitimate cases, but was unwilling to be public about the issue and thus did not seek administrative relief. Instead the administration chose a secretive and unsettling solution: authorizing warrantless wiretaps between targets abroad and those with whom theycommunicate inside the United States. Secrecy might have prevented the program from ever coming under judicial scrutiny but much to the administration's distress, the program was leaked to the *New York Times* (Risen and Lichtblau 2005), which published it in the fall of 2005.[35] Suit was brought against the NSA and its director by the ACLU and numerous co-plaintiffs. In August of 2006, the plaintiffs won their first battle. Judge Anna Diggs Taylor of the Eastern District of Michigan, Southern Division, ruled that the government's program was both a violation of the Foreign Intelligence Surveillance Act (which limits as well as enabling wiretapping) and of the constitution, which prohibits unreasonable searches and seizures (*American Civil Liberties Union et al. v. National Security Agency et al.* (United States District Court Eastern District of Michigan Southern Division, Case No. 06-CV-10204, Hon. Anna Diggs Taylor, *Memorandum Opinion*.)).

One category of communications seems to deserve special consideration. *Transit traffic* is traffic that enters the US only to go on through and come out the other side. Because the communication system of the US is so well developed and because the US is responsible for such a large fraction of the world's commercial activity, it is not surprising that a significant fraction of the communications from Europe to the Far East go via the United States.

How should we treat such communications? Our signals intelligence service is pleased to build antennas on US soil whenever this will give them satisfactory reception, without worrying that once the signal hits the antenna it is in the US and subject to the protection of US law. Are

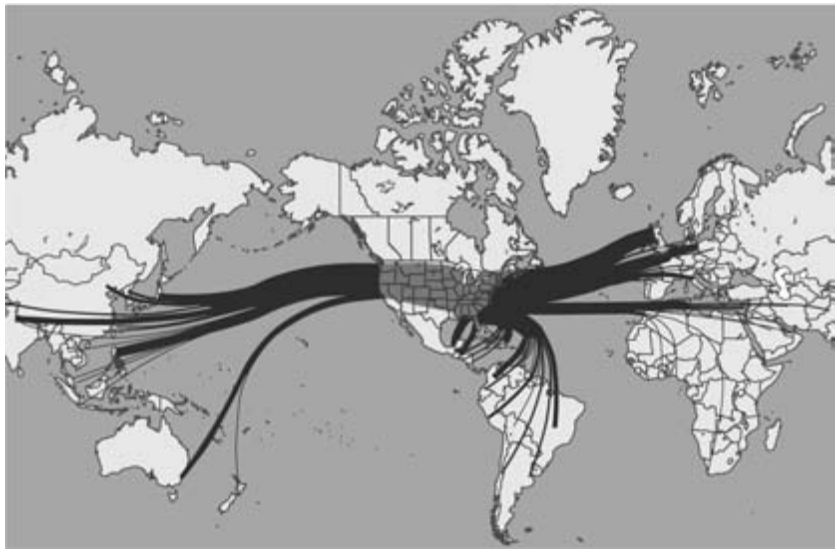


Figure 11.2
Worldwide telecommunications flows.
(Illustration by Nancy Snyder.)

signals that come in on wires different? The NSA did not think so and at some point began collecting the transit traffic.

Another area of contention is information *about* communications, what is called *call detail recording*. The US telecommunications companies have a long history of handing over communications and associated records to NSA and its ancestors. In 2006, a new manifestation of this practice surfaced; most of the country's major carriers were giving NSA the call detail recording (essentially billing) information on their customers, even for calls that originated and terminated entirely within the US. The action did not go unchallenged. The lawyers of the Electronic Frontier Foundation brought suit "on behalf of themselves and all others similarly situated" seeking declaratory and injunctive relief from the federal courts against AT&T (and some 20 "Does") (*Tash Hepting et al. v. AT&T Corporation et al.*, United States District Court for the Northern District of California, Case 3:06-cv-00672-vrw).

Although call detail recording falls far short of content interception for many purposes, for others it is more useful because it provides a window into the past. It parallels the electrical engineering practice of watching a signal with a delay line; triggering observation on the basis of something

that happens later; and then looking back at the signal in the delay line to see what happened earlier.

Suppose that on March 1 there is a bombing. On March 2, a well-known radical makes a public statement on the subject, or calls a targeted suspect, or flies out of town. Investigators with access to the radical's old phone records now look to see whom she called in the previous week, two weeks, month, a year. These queries will lead to yet other queries about earlier calls, queries that take into account the location of the bombing, calls to travel agencies or airlines, calls to other people under investigation. It would of course be useful to have all of the communications of the people under investigation but, legal issues aside, it is generally infeasible to record such large volumes of traffic.[36]

Changing US Role in the World

The United States, with only a few percent of the world's population, has long been accustomed to being its dominant economic and military power and one of its major cultural powers. With the rising wealth, as well as population, of China and India, and the increasing unification of the European Union, all this is likely to change.

Despite the ambitious and surprisingly internationalist cryptographic standardization program being undertaken in the US the new generation of American-sponsored cryptographic systems may have less influence today than DES did a generation ago. Europe has undertaken a broad program to develop cryptographic tools to support its information security needs.[37] China has also undertaken the development of new families of cryptographic systems, but if these are public within China, which seems doubtful, they have not made it to the west.

Among the most profound changes that will affect privacy and security policy is the increasing virtualization of computers. At present, the nominal basis of computer usage is the personal desktop or laptop computer computer—a moderately large, moderately expensive and very capable device that can execute billions of instructions a second and store tens of gigabytes of data. The great growth areas in computing, however, are above and below this. On one hand enterprises like Google supply computing services to their customers from computing engines built out of the better part of a million rack-mounted PCs. On the other the tool

that people use to access this resource is ever more likely to be a palmtop rather than laptop computer—something small enough to carry everywhere and just powerful enough to serve as your gateway to the Internet.

In a world of virtual computing neither individuals nor organizations will be able to have the sort of security they have been accustomed to in the past. When powerful computations can be done for you by specialized providers more satisfactorily and less expensively than you could do them yourself, use of such services will become a way of life. In order to use them, however, you must accept a breach of security comparable to using an unencrypted radio. If you ask for services, there is no way of concealing what you want done, just as there is no way of getting Google to search on your queries without revealing what your interests are.

The popularity of the MMORPGs points the way to another level of this development. If your major way of interacting with other people is though virtual environments, you will be able to augment yourself with capabilities undreamed of in the past. In a virtual world no one will know whether you are a dog with a prodigious memory or whether you are a dog that is really skillful at typing fast Google queries. In this world a matter that has concerned us since our first chapter comes to the fore. We noted that things that had been facts of life became subject to social policy. In the virtual world, this will be true of almost everything.

Yet What Exactly Is the Terrorist Threat?

Law-enforcement's view of what works in terrorist cases was summed up in 1991 by FBI Director William Sessions: "If a terrorist attack does occur, it is our view that a swift and effective investigation culminated by arrest, conviction and incarceration is a powerful deterrent to future acts of terrorism." (Sessions 1991, p. 72) Thus through the 1990s and into the current decade, the law-enforcement community has pushed for tools that enable investigations that end in "arrest, conviction, and incarceration."

Not everyone in law enforcement agrees with Sessions's approach. During hearings on the USA PATRIOT Act, Associate Deputy Attorney General David Kris said: "And just as a tactical matter, sometimes prosecution is not the right way to go. Other times you just want to monitor these people or do something else. You try to recruit one of

them as a double agent. You feed them false information. You disrupt them using some other technique," even while, "In some cases you do want to prosecute." (Kris 2002, p. 28)[38]

The passage of 15 years reveals that Sessions's statement does not encompass the current terrorist threats. Terrorists, even those who do not sacrifice their lives in the act of terror as the 9/11 hijackers did, seem undeterred by the prospect of prosecution. Timothy McVeigh, convicted of the 1995 bombing of the Murrah Federal Building in Oklahoma City, accepted execution with an observation that might have been written by a spokesman for the US military. The body count was in his favor: he had killed 168; they would kill one.

In the disorienting days immediately after 9/11, it was easy to forget that such attacks had been anticipated. In addition to the now-famous memo of August 2001,[39] there were investigators in both the FBI and the CIA who had been tracking bin Laden and other terrorist groups. There were also various studies of the security of the United States in the post Cold War era. Perhaps the best known is the report of the United States Commission on National Security/21st Century, more commonly known as the Hart-Rudman report, after the two former senators who co-chaired the committee.[40] Seven months before the 9/11 attacks, the Hart-Rudman report observed that the US would become "increasingly vulnerable on the America homeland" and that the US military would not be fully able to stop the threats. They went on to say:

> We believe that American strategy must compose a balance between two key aims. The first is to reap the benefits of a more integrated world in order to expand freedom, security, and prosperity for Americans and for others. But second, American strategy must also strive to dampen the forces of global instability so that those benefits can endure and spread.
>
> . . . the United States should . . . promote pluralism, freedom of thought and speech, and individual liberty. Not only do such aims inhere in American principles, they are practical goals as well. There are no guarantees against violence and evil in the world. We believe, nonetheless, that the expansion of human rights and basic material well-being constitutes a sturdy bulwark against them. On the negative side, these goals require concerted protection against four related dangers: the proliferation of weapons of mass destruction; international terrorism; major interstate aggression; and the collapse of states into internal violence, with the associated regional destabilization that often accompanies it. (Hart et al. 2001, p. 5)

In considering the terrorist threat, the issue at hand is that wiretapping has non-monetary costs. Creation of a surveillance society will quickly be negatively perceived in some immigrant communities both because such societies are what they sought to escape in coming to the US and because they perceive themselves as the explicit targets of surveillance. The effective imposition of surveillance threatens innovation and security by building wiretapping capabilities directly into communications infrastructure. Such costs must be undertaken cautiously and require asking, "What is the value of wiretapping in terrorist investigations?"

The current most serious threat of terrorism, at least in terms of large-scale attacks, comes from violent Islamic fundamentalists, people who look at a war in terms not of years but of centuries (Fallows 2006, p. 60). Investigation of this threat will need the cooperation of domestic immigrant communities (Heymann 1998, pp. 101-102). The threat posed by sleeper cells is particularly serious and the need for community cooperation in uncovering them is acute. As London Police Commissioner Ian Blair put it, "The whole deal here is to engender the trust that one afternoon may allow one of those Islamic leaders to say to the sergeant, 'You know, I'm worried about young so-and-so.'" (Caldwell 2006b, p. 44). The investigation into the 2006 London airline threat began with just such a tip from "several people in Walthamshow," the East London home of some of those accused (Van Natta 2006, p. A8).

Experience with terrorist investigations in Israel and Northern Ireland shows that harsh techniques—massive searches and surveillance, ill-treatment and abuse of prisoners—often backfire (Heymann 1998, pp. 132, 141–142). In Northern Ireland the advantages gained through this type of policing appeared to have been "offset by the effect of stimulating IRA recruitment" (ibid., p. 126). In this light, the US government's early response to 9/11: singling out young male immigrants from Islamic nations and subjecting them to extensive questioning by the Immigration and Naturalization Service when there was no *a priori* suspicion of wrongdoing was counterproductive.[41]

Arab and Muslim immigrant populations in the United States have assimilated—second-generation American Muslims "are culturally and economically Americanized" (Fallows 2006, p. 65)—while European immigrants have not.[42] According to former of the National Security Council member Daniel Benjamin, American Muslims "have been our

first line of defense" (ibid., p. 65) since 9/11. They are a resource to be treated with care.

The construction of a surveillance society, and particularly surveillance in Muslim communities, may well be counterproductive. Government policy can go two ways: it can work to create trust[43] or it can build a surveillance society that many in the Muslim community see, with some justification, as targeting them. As Phillip Heymann, former US Deputy Attorney General, has observed, the latter direction has very serious dangers: "In terms of national well-being, the gravest national dangers from a terrorist act (short of an immense escalation of terrorist tactics), are that the interplay of terrorism, public reaction, and governmental response may sharply separate one significant group from the rest of society." (Heymann 1998, p. 2) In such situations, Heymann notes, "the terrorists will find it far easier to secure communication channels, [etc.]" (ibid., p. 13). The lawyer of the LA 8, David Cole, described the FBI pursuit of the seven men and one woman as costing the US government heavily in ways the government could hardly afford to pay: "[T]he L.A. 8 case, seen in Arab-American communities as the prime example of US hostility toward Arab immigrants, has probably done more to undermine that effort than any case in the past 20 years. . . .The vendetta against the L.A. 8 was a critical reason for the Arab community's deep distrust of the government even before 9/11." (Cole 2003)

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

While the threat of prosecution is a deterrent to members of organized-crime groups, it is much less effective against those espousing violence as a way to achieve a fundamentalist society. Heymann has observed that law enforcement is not a deterrent to terrorists (1998, p. 79). Quite the contrary: violent Islamic fundamentalists often view jails as excellent re-

cruiting grounds—including among the nationals in the country in which the terrorism is to take place.

Let us be clear: we are not arguing that wiretapping and signals intelligence are without value in terrorist investigations. They have proved their value time and again and the very threat of interception has severely impeded al-Qaeda operations. The organization has learned the danger of communicating electronically, and Osama bin Laden is said to rely on handwritten messages delivered by trusted couriers rather than use the telephone. This represents a serious meaconing of al-Queda's communications directly attributable to US intercept capabilities. Many terrorist communications, however, are sufficiently brief that they are difficult to decipher not because of they are electronically encrypted but because the communications are in "code" known to the insiders but not to the eavesdroppers.[44] Our concern is that in as much as wiretaps are not free, either in their impact on immigrant communities or their impact on network architecture, they are also not an investigative panacea.

Traffic flow information is often as valuable as content and it is much harder to conceal. Investigators have been quite successful in tracking terrorists without being able to learn the contents of their messages. In a 2002 case, 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 cards (Van Natta 2004, p. A1). The result was the arrest of a number of operatives and the breakup of al-Qaeda cells.

This example illustrates what the intelligence community has known for years. In the age of electronic communications, analyzing the content of communications is a rich and fruitful investigative tool when you can get it but developments ranging from the low cost of optical fiber to the critical need to secure civilian infrastructure has made the contents of intercepted communications ever more frequently inaccessible.[45] Traffic analysis—who is communicating with whom, for how long, on what kind of channels, and in what volume—is the more fundamental tool. Traffic analysis reveals an organization's structure, its membership, even the roles of its members. Traffic analysis has another, extremely impor-

tant benefit; it is a tool that aids investigators without requiring security breaches in on the civilian infrastructure.

It is important to apply common sense to the issue of terrorist investigations and to think clearly about which acts can be prevented and which cannot (Heymann 1998, pp. xxi–xxiii). Timothy McVeigh's attack on the federal office building in Oklahoma City was the work of a group of three people. The al-Qaeda attacks of September 11 involved the coordination of a group six times that size but still quite small. Unless the United States moves to a surveillance society on the scale of the former East Germany, the country will never be able to protect itself fully against attacks by "lone warriors" such as McVeigh. We need to factor such common sense into all of our thinking about security.

We also need to have clear understanding of how serious the threat of international terrorism to the domestic United States actually is. Despite government classification of much of the information, there is some data publicly available which can clarify some of these issues. In June 2006 the US Department of Justice released a *Counterterrorism Whitepaper* detailing investigative successes in terrorism cases (ibid. 2006). This report stated that in the period from 9/11 to June 2006, there were 441 defendants charged with terrorism or terrorism-related activity of an international 'nexus' (ibid., p. 13). But this data is not all that it seems. To be sure, the report included a number of serious cases: the indictment (on charges of providing material support to a terrorist organization) of four associates of Sheikh Omar Abdel-Rahman, who had himself been convicted in 1995 for his role in the first attempt to destroy the World Trade Center (ibid., p. 16); the conviction of Zacarias Moussaoui; the indictment and conviction of Richard Reid, the "shoe bomber."[46] But the DoJ report also highlighted a number of lesser cases, including the Florida case of Narseal Batiste and associates, accused of plotting to blow up the Sears Tower in Chicago (ibid., p. 64), but which is now considered a "pipe dream," a "quixotic" effort by the plotters, who were led by an FBI informer (Pincus 2006, p. A1). Other cases detailed in the report include that of a husband in possession of ricin, possibly for use in poisoning his wife because of her extramarital affair (USDoJ 2006, pp. 24–25), a case which began with the premise of foreknowledge of 9/11 by a group of stockbrokers and ended with a simple case of racketeering

and securities fraud (ibid., p. 19), and various ones of much lesser import, such as visa violation and marriage fraud.

The DoJ report should be contrasted with the analysis of criminal terrorism enforcement by the Transactional Records Access Clearinghouse (TRAC) in September 2006 (TRAC 2006).[47] The TRAC analysis, based on information from the Department of Justice's Executive Office for United States Attorneys (EOUSA) compiled on a monthly basis, shows quite different results than the official *Counterterrorism Report*. From July 2001 through May 2006, the government prosecuted 335 people as "international terrorists" (ibid.). As we shall see in a moment, few of these cases were actually terrorist cases. In any case, this is a somewhat different number than the DoJ report, which had lumped together international terrorists, such as Abdel-Rahman, Moussaoui, and Reid, with domestic actors (violent anti-abortion activists, members of the Ku Klux Klan, right-wing militias, and the like). While the latter have been and remain a serious concern—until 9/11 the most serious recent[48] act of terrorism within the domestic United States was carried out entirely by domestic terrorists (Timothy McVeigh et al.)—the current area of concern is international terrorism. Because the TRAC numbers are based on EOUSA data that does not include names, it is difficult to directly reconcile the two reports.

The TRAC data is the hard numeric data compiled by US attorneys. In many ways, the difference between the DoJ and TRAC reports parallels the difference between 1994 Freeh testimony to Congress regarding the efficacy of wiretaps and the later analyses of the Wiretap Report produced by the Administrative Office of the US Courts. The former discussed the value of wiretapping in kidnapping cases[49] —a conclusion that a study of the Wiretap Report did not support[50]—and lumped together all electronic surveillance results. Since electronic surveillance includes bugging—and some of the most important convictions, including Gotti's and Stanfa's came about because of electronic bugs and *not* wiretaps—this imprecise information was far less useful—and far more politically motivated—than the results that came from a careful study of the Wiretap Reports.

TRAC's hard data had some very interesting results. There is a surge in federal prosecutions of international terrorism cases in the year imme-

diately after 9/11, but a recent return to pre 9/11 levels. There were 213 convictions in international terrorism cases between July 2001 and May 2006. Of these, 123 individuals received prison sentences, but most convictions were not for serious crimes. Only fourteen individuals received sentences of five years or more, and only six of these received sentences of twenty years or more (TRAC 2006). From the vantage point of 9/11, the bombings in Bali, Madrid, and London, it is clear that there is a serious worldwide terrorism threat from violent Islamic fundamentalists; the data from the TRAC report puts that threat in a clearer perspective. As TRAC asks "Is it possible that the public understanding about the extent of this problem [of international terrorism] is in some ways inaccurate or exaggerated?"

Maybe the focus in communications should be elsewhere? We must be prepared for the possibility that we will not be able to prevent terrorist attacks from occurring in the United States and must, therefore, develop infrastructure to enable recovery—whether it is from natural disasters or man-made ones. In that, the lessons of both 9/11 and Hurricane Katrina demonstrate a clear need for interoperable and robust communications systems. The aim of avowed terrorists to cause the greatest possible disruption of society argues against creating centralized resources whose loss would be crippling. In the physical world this argues for distributed sources of energy, manufacturing, and food. In communications it argues for security in depth. A system in which there is no all pervasive mechanism that can provide or deny security at will, may give an opponent unintended access to communications and computing throughout a national network. These may be the concerns that caused the national-security agencies to support changes in standards and export control regulations to encourage widespread use of strong encryption.

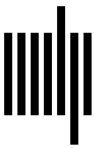
Privacy on the Line

The Politics of Wiretapping and Encryption

By: Whitfield Diffie, Susan Landau

Citation:

Privacy on the Line: The Politics of Wiretapping and Encryption
By: Whitfield Diffie, Susan Landau
DOI: 10.7551/mitpress/5572.001.0001
ISBN (electronic): 9780262256018
Publisher: The MIT Press
Published: 2010



The MIT Press

Composed in LaTeX 2_ε by the authors.
Set in Sabon by Loyola Graphics of San Bruno, California.
Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Diffie, Whitfield.
Privacy on the line : the politics of wiretapping and encryption / Whitfield Diffie, Susan Landau. — Updated and expanded ed.
p. cm.
Includes bibliographical references and index.
ISBN 978-0-262-04240-6 (hardcover : alk. paper)

1. Electronic intelligence—United States. 2. Wiretapping—United States. 3. Data encryption (Computer science)—Law and legislation—United States. 4. Electronic surveillance—United States—Political aspects. 5. Telecommunication—Political aspects—United States. 6. Privacy, Right of—United States. I. Landau, Susan Eva. II. Title. III. Title: Politics of wiretapping and encryption.

UB256.U6D54 2007
342.7308'58—dc22 2006035514