8

Communications in the 1990s

Briefings on the dangers of encryption by Raymond Kammer (the acting director of the National Institute of Standards and Technology) and Clinton Brooks (assistant to the director of the National Security Agency) gave rise to fear in the FBI that wiretaps would soon be rendered useless. In 1992 the FBI's Advanced Telephony Unit predicted that, because of encryption, by 1995 the FBI would have access to only 60% of intercepted communications.[1] Facing a technology it understood poorly, the FBI wanted a fast remedy. As a first step, it sought congressional action to protect wiretapping from technical encroachments. The idea was that, because wiretapping was a tool with accepted legal standing, new legislation could be presented as a matter of maintaining the status quo.

Digital Telephony

Unless continued access to traffic is maintained, neither targeting nor analysis of electronic communications will be possible. The post-1982 breakup of AT&T presaged a period of tremendous growth in telecommunications products and businesses. For the FBI's wiretapping activities, it was a period of growing complexity. In executing wiretaps, agents could no longer deal with a single telephone company; they now had to deal with equipment supplied by a variety of companies and with service provided by numerous carriers.

In 1992 the FBI put forth what it called a Digital Telephony Proposal, which mandated the inclusion of provisions for authorized wiretapping in the design of telephone switching equipment. When the FBI

approached Congress with that proposal, it was far from clear that the FBI was experiencing anything other than a crisis of confidence. The proposed bill required that all telecommunications providers, both public carriers and private branch exchanges (PBXs—the private switching centers typically used within large companies), design their systems to accommodate government interceptions. Common carriers had 18 months to comply; the PBXs had twice as long. All costs of redesign were to be borne by the companies (FBI 1992b). The FBI claimed that new switching technology and such improvements as cellular telephones and call forwarding had made it difficult to install court-authorized wiretaps.

Evidence to substantiate that claim was hard to find. On April 30, 1992, the *Washington Post* reported: "FBI officials said they have not yet fumbled a criminal probe due to the inability to tap a phone. . . ." (Mintz 1992) To this suggestion that it was not actually having any trouble, the FBI countered that, because of anticipated technological problems, court orders had not been sought, executed, or completely carried out (Denning et al. 1993, p. 26). Meanwhile, Freedom of Information Act litigation initiated by Computer Professionals for Social Responsibility found not a single example of wiretaps' being stymied by the new telecommunications technology.

Industry objected to the Digital Telephony Proposal and major players in computers and communications protested. Among industry's concerns were the cost (estimated to be in the hundreds of millions of dollars[2]) and the effect on privacy. A built-in "back door" for government wiretapping could easily become a back door to illicit surreptitious surveillance.

The General Accounting Office briefed Congress, expressing concern that alternatives to the proposal had not been fully explored (USGAO 1992). The General Services Administration characterized the proposal as unnecessary and potentially harmful to the nation's competitiveness (USGSA 1992). In an internal government memo, the National Telecommunications and Information Agency observed that facilitating lawful government interception also facilitated unlawful interception by others, and described the bill as "highly regulatory and broad" (NTIA 1992).[3] There were no congressional sponsors for the proposal.

As internal memoranda show, the FBI had given the Digital Telephony Proposal only a 30% chance of passing (McNulty 1992, p. C-14). But the proposal established an FBI beachhead.

The Value of Wiretapping

The Digital Telephony Proposal took as given the proposition that wiretaps were essential to law enforcement. Wiretapping for that purpose had been legal for a quarter of a century and, despite the fact that most Americans disapproved of it,[4] had come to be an accepted practice.

Decades of court-authorized wiretapping have provided a powerful analytic tool with which to assess its value: the reporting provision of Title III provides that the Administrative Office of the Federal Courts should annually publish a list of all wiretap orders issued under Title III and associated state statutes. This annual account is commonly known as the *Wiretap Report*, although, like Title III itself, it covers all forms of electronic surveillance, including microphone surveillance. Despite its value as an analytic tool, the *Wiretap Report* has severe limitations. In its statistical summaries it does not distinguish wiretaps from bugs. Another difficulty is establishing precise numbers. For example, in its statistical information on intercepts, the report uses the term "intercepts installed" to mean installed intercepts for which reports have been received. This probably results in a slight underestimate of those actually installed, since some are not subsequently reported upon. The 1988 report shows that there were 754 orders for electronic surveillance but indicates that 11 of these were never executed. Of the remaining 743 court orders, an additional 67 did not have an after-the-fact prosecutor's report.[5] Thus the report lists 676 "intercepts installed," although the actual number lies between 676 and 743. In our analysis, we have used the *Wiretap Report's* "intercepts installed" figure, as there is no way to ascertain the higher number.

Limitations of the Data

From the *Wiretap Report* we can discern who the prosecutor was on a wiretap order, who the judge was, how long the order was for, and for what crime the order was authorized.[6] We can see how many arrests were made and how many convictions occurred.[7] What we cannot discern from the *Wiretap Report* is what was said in the court hearings.

Court transcripts often reveal information that dry numbers hide. In 1972, law professor Herman Schwartz studied the 4 years' worth of court-ordered wiretaps that had resulted from Title III. He observed:

> [T]here is an interesting item in the late J. Edgar Hoover's 1971 [FBI annual] report: right after a reference to the vital importance of electronic surveillance to the fight against organized crime, four major convictions are listed, including one of a Nicholas Ratteni. A check with counsel in the case disclosed that there was indeed a wiretap—against a co-defendant who was *acquitted*. (Schwartz 1974, pp. 186–187)

So the FBI dissembled. Schwartz uncovered a number of other results that undercut claims of wiretapping's usefulness:

> [I]n *United States versus Poeta*, the US Court of Appeals opened its opinion by observing that the tap-derived evidence was unnecessary to the conviction; in another case, *Uniformed Sanitation Men versus Commission of Sanitation*, the Court made the same observation. In a 1971 report, a Nevada prosecutor reported two indictments in a kidnapping case in which wiretapping was used … but candidly added that the indictments were "not as a result of the interception." (Schwartz 1974, pp. 185–186)

The law requires that the number of interceptions, both incriminating and non-incriminating, be reported. Schwartz found that law-enforcement personnel were prone to exaggerate the number of incriminating intercepts:

> In *United States v. King*, the Government claimed that 80–85% of the conversations overheard in a drug case were incriminating and so it reported in the 1971 report, Order #35. The Court, however, found that the contemporaneous reports showed that the percentages were really between 5 and 25%.[8]

Naturally, such anomalies continue, of course. One enterprising New York lawyer has used wiretaps made by police to argue that his client had been entrapped.[9] In a 1995 terrorist conspiracy case, the FBI worked hard to establish a connection between Sheik Omar Abdel Rahman (a blind Egyptian cleric living in Brooklyn) and Razmi Yousef (an alleged terrorist and bomb expert). The FBI emphasized the wiretap evidence. In fact the wiretap transcripts only revealed that there had been several calls between Rahman's phone and Yousef's (Fried 1995; McKinley 1995b)—something that could have been discovered by less intrusive investigative methods. Both Rahman and Yousef were involved in terrorist activities but they never spoke to each other on the tapped telephone. Wiretaps of Rahman's conversations were described in the above-cited *New York*

Times stories as "not incriminat[ing]" and containing "no references to violence." In a situation reminiscent of the Ratteni case described by Schwartz, lawyers for the defense in the 1997 trial of Timothy McVeigh used wiretaps made by federal agents to demonstrate that a prosecution witness was unreliable (Brooke 1997b).[10] Such examples make clear that the data provided by the *Wiretap Report* give only a partial picture of wiretapping cases.

Where Wiretaps Are Used

Here is how things stood in the mid 1990s, as the Communications Assistance for Law Enforcement Act and encryption were being debated.

In 1968, wiretapping was seen as a tool for targeting gambling—the main source of income for organized crime. In the first 5 years after the "Title III" legislation, 64% of the 2362 reported intercepts were for investigations of gambling cases, 27% of the wiretaps were for narcotics cases, less than 5% for homicide and assault investigations, 2.5% for investigations into bribery, and under 1% for cases of "arson and explosives" (AO 1978, p. xvi). (The *Wiretap Report* denotes as "narcotics" any case in which the most serious offense includes drugs of any sort, including marijuana.) With at least 38 states running lotteries, and gambling legalized from Connecticut to Nevada, it is difficult to recall that gambling was once targeted as a serious crime.

In 1977 the number of narcotics investigations employing electronic surveillance began increasing. In 1982 President Reagan declared a national "War on Drugs," and gambling investigations using electronic surveillance dropped while narcotics investigations rose. In 1994 narcotics investigations made up 77% of the cases using electronic surveillance, gambling investigations less than 8%. Cost is a limiting factor. The average cost of a wiretap has risen, from $1358 in 1968 to $49,478 in 1994; part of this increase was due to a doubling in the length of the average electronic surveillance, from approximately 20 days in 1969 to just under 40 in 1994. Drug investigations, which frequently involve wiretaps of several months' duration, are particularly costly.

Drug investigations are the major focus of wiretaps and the seizure of major shipments of drugs is sometimes accomplished through their use. In a style similar to the Vietnam War's body counts, law-enforcement

agencies set great store by the tonnage of drugs seized. However, not even the law-enforcement community is unanimous in believing that seizure is the best solution to the drug problem. Eliminating drug sources has had only limited success.[11] And money spent on drug busts may not be money well spent. A report prepared by a special committee of the American Bar Association concluded: "While law enforcement has had little effect on drug use, drug prosecutions have had a profound effect on the criminal justice system. In the cities the Committee visited, drug cases have overwhelmed the courts. . . . In light of the Committee's findings in the area of drugs, a simple but significant truth should be faced: conventional law enforcement methods are not controlling the drug problem." (American Bar Association 1988, pp. 46–47)

Sample Data from the *Wiretap Report*

Court-Authorized Electronic Surveillance, Title III, 1988–1994								(1994 Only)	
Year	1988	1989	1990	1991	1992	1993	1994	Federal	State
Orders Authorized	738	763	872	856	919	976	1154	554	600
Orders Denied	2	0	0	0	0	0	0	0	0
Orders Installed[1]	678	720	812	802	846	938	1100	549	551
Main Offense[2]									
Arson, Explosives, and Weapons	3	0	0	0	0	0	0	0	0
Gambling	126	111	116	98	66	96	86	8	78
Kidnapping	1	3	2	5	9	1	11	7	4
Narcotics	435	471	520	536	634	679	876	435	441
Racketeering	80	89	90	114	90	101	88	68	20
Telephone Wiretaps[3]	549	621	591	591	632	679	768	397	371
Electronic Bugs[4]	61	65	62	62	38	55	52	42	10
Average Number / Order									
Persons	129	178	131	121	117	100	84	112	58
Intercepts	1251	1656	1487	1584	1861	1801	2139	2257	2030
Incriminating Intercepts	316	337	321	290	347	364	373	374	372

1. *The Wiretap Report* uses the term 'Intercepts Installed' to mean intercepts installed *and* reported upon. This is likely to be a slight underestimate of those actually installed, since some surveillances are not actually reported upon. We use the Administrative Office's terminology here.
2. As determined by judge issuing surveillance order.
3. This number does not include telephone wiretaps that were part of a "combination" tap involving more than one type of surveillance.
4. This number does not include electronic bugs that were part of a "combination" tap involving more than one type of surveillance.

While wiretaps may contribute to large drug busts (although we are not aware of any study that has compared employing wiretapping with

spending comparable funds on other types of law-enforcement activities focusing on drugs), it is not clear that this effort makes any real difference in the underlying problem. Indeed, a 1994 RAND study observes that $34 million invested in drug treatment programs achieves the same consumption reduction as does $246 million spent for domestic law enforcement, $366 million spent for interdiction, or $783 million spent for source-country control.[12]

Where Wiretaps Are Not Used

Although kidnappings are frequently touted as a reason for the need for electronic surveillance,[13] wiretapping does not seem to be useful in such cases. Between 1969 and 1994, wiretaps and microphone bugs were reported to have been used in 80 kidnapping cases; thus, on average, wiretapping played a role in two to three of those cases each year.[14] Though there is no reason to doubt that the court orders for surveillance were correctly made, there is some reason to doubt the necessity. Meanwhile, in recent years there have been approximately 500 kidnapping cases per year.[15]

It is not surprising that wiretaps rarely figure in kidnapping cases, since investigators are typically unaware of the kidnappers' locations. But wiretapping's role is small for another reason: the interception of ransom calls from kidnappers does not require any court authorization if the recipient of the call consents—a form of interception called a "consensual overhear."[16]

Domestic terrorism is sometimes given as a reason for wiretap surveillance. There were 59 wiretapping cases between 1968 and 1994 involving arson, explosives (the most frequent form of domestic terrorism), and weapons, or about two a year. The period 1988–1994 saw four Title III wiretap investigations of firearms and none of arson or explosives.[17] It is possible that no wiretaps were used in cases involving explosives. However, since intelligence wiretaps may also be used for investigating domestic terrorism if there is alleged foreign involvement, it seems more likely that federal authorities found it more expedient to employ the Foreign Intelligence Surveillance Act, under which nothing need be reported but the total annual number of surveillances.

The States and Wiretapping

Forty-four states have their own wiretapping statutes, but not all of those states strongly support wiretapping. It took California more than 20 years to pass a wiretapping statute, and when the law finally did pass it was loaded with restrictions, including a limitation to drug investigations. At first the state of California performed few wiretaps a year—8 in 1994 compared to 71 federal wiretaps (AO 1995, pp. A-2–A-7 and A-58). "If it's anything big, you should let the Feds do it," explained San Francisco Chief Assistant District Attorney Dick Iglehart, who was California's Chief Assistant Attorney General, Head of the Criminal Division, at the time of the passage of the California statute.[18] By 2004 California had caught up with New York and the other big players, and had performed 180 state investigations using wiretaps. Over half of those were in Los Angeles, where there was reason to believe that there had previously been substational underreporting of state wiretaps.[19] The Public Defender's office filed suit over the practice, and a Los Angeles police officer testified that the hand-off procedure was standard practice and had been used "hundreds of times" since the mid 1980s with "10 percent to 15 percent of the cases involving wiretaps concealed from the defense" (*New York Times* 1998b). Despite strong objections from the Public Defender's office (Quant 2006), the judge ruled that the hand-off was permissible. But then something very interesting happened regarding the number of state wiretaps reported for Los Angeles. Despite the Superior Court ruling and the LAPD claim that the practice was "standard procedure," the number of legally-authorized state wiretaps in Los Angeles jumped from 37 in 1998 (AO 1999, p. 14) to 62 in 1999 (AO 2000, p. 15) and then 78 in 2001 (AO 2002, p. 15). It is, or course, impossible to know what fueled this increase: better reporting, or a real increase in the number of state wiretaps. The *Wiretap Report* reports 48 jurisdictions that permit wiretapping: the Federal, Puerto Rico, the Virgin Islands, the District of Columbia, and 44 states.

Convictions from Wiretaps

How many convictions result from wiretaps?[20] In 1988 wiretaps were used in 609 investigations, including 45 in which both wiretaps and

electronic bugs were employed. There were 279 court cases and 1808 convictions in these cases.[21] These convictions had cost $335 million for wiretapping alone.

Of course, it is impossible to know in how many of these cases wiretap evidence was crucial in obtaining a conviction or a guilty plea (whether directly or through evidence obtained as a result of the information gleaned from a wiretap). The numbers above provide only an upper bound on the potential effectiveness of wiretapping in law enforcement. It is essential to note that a wiretap is ordered only if there is already probable cause that the person being investigated is involved in a serious and indictable crime.

Who Else Is Being Tapped?

Since Title III has been in force, the number of conversations intercepted has increased, the number of nonincriminating conversations intercepted has increased, and the number of incriminating conversations intercepted has remained the same. More specifically, according to data on the period 1968–1994 released by the Administrative Office of the US Courts, the average annual number of incriminating conversations intercepted remained between 200,000 and 400,000 per year, while the number of intercepted conversations increased steadily from about 400,000 in 1968 to over 2 million.[22] In 1994, for example, 1137 court orders for electronic surveillance resulted in the interception of 2.35 million conversations. Only 15% of the intercepted conversations were incriminating; the remainder of the wiretapped conversations were not related to illegal activities.[23]

Gambling accounted for 29% of the incriminating wiretap intercepts in 1994. Gambling skews the statistics, for it is an activity with a high number of incriminating intercepts. It is also low on convictions. If we look to the 1988 numbers now that there has been enough time for trials to have taken place, we see that gambling accounted for 27% of the incriminating wiretap intercepts but for less than 14% of the convictions (244 of 1808). It is not surprising that wiretaps authorized for a gambling investigation should yield incriminating calls, since there has to be probable cause for the authorization. Neither is the low level of convictions a

surprise; if a bookmaking operation is tapped, the incriminating calls are likely to be people placing bets. Few, if any, of these low-level bettors are prosecuted.

Thus, from the raw data of the *Wiretap Report* we can observe that fewer than one-sixth of the intercepted calls resulted in anything of use to law enforcement.

How Things Stand Now

The numbers above describe the situation in 1998, when this book first appeared. With only minor exceptions, things have not changed substantially in the past decade. Except for a dip in 2000, the number of Title III wiretaps continues to rise, with 1773 Title III wiretaps reported by the Administrative Office of the US Courts for 2005 (AO 2006, p. 7). There has been a shift, with state and local wiretaps constituting an ever-increasing percentage of Title III wiretaps. Undoubtedly one reason for this shift is the number of wiretaps from the state of California, which was 235 in 2005; New York, with 391, New Jersey with 218, and Florida with 72 make up 80% of the state applications for wiretap orders (ibid., p. 7). In 2005, fully 81% of all Title III wiretaps were for drug cases (ibid.), up slightly from the 72%–77% range of previous few years. The average wiretap in 2005 cost $55 thousand, lower than the cost in 2004, and wiretaps were used for an average of 43 days (AO 2006, p. 9). As had been the case previously, contrary to public testimony, wiretaps are not particularly efficacious in kidnapping cases. Over the last nine years, wiretaps have been sought in an average of only five kidnapping cases a year and installed in an average of fewer than four kidnappings a year (AO 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006).

Two changes do stand out, however. The first is the move to portable devices. In 2001, the most common devices being wiretapped were portable devices (AO 2002, p. 8). To no one's surprise, that trend has continued. The second change from the mid 1990s is not unrelated to the first. Portable devices have driven an increase in the number of daily communications. So it should also be no surprise that the government is conducting surveillance on an increasing number of communications. In 2004, the number of intercepted communications under Title III was

a record 4.9 million, slightly over a million of which were deemed incriminating (AO 2005, p. 21). In 2005, the government's success ratio improved slightly: the number of interceptions was down to 4.8 million, while the number of incriminating ones was slightly higher that it had been in 2004, so that 22% of communications tapped under Title III warrants were incriminating (and 78% were not).

In 2000 Congress extended the reporting requirement for the Administrative Office of the US Courts, which was due to expire and added a twist: reporting on encryption problems encountered during wiretapping cases.[24]

Reports were to be aggregated, so that there would no break-out of the cases in which law enforcement encountered encryption. The result is quite different from what the FBI had anticipated in 1992, when the Advanced Telephony Unit predicted that it expected fully 60% of wiretapped calls would be encrypted (Advanced Telephony Unit). Law enforcement has encountered encrypted communications. There were 22 state and local cases in 2000, 34 state and local cases in 2001, 17 state and local cases in 2002, one state case in 2003, 41 state cases and one federal case in 2004, and 13 in 2005. Of these exactly one caused difficulty and the ciphertext could not be decrypted.

What has given rise to these curious figures is hard to determine.[25] Another oddity is that federal investigators, seemingly more likely to encounter encryption than state and local investigators, reported encountering only a single case of encryption. Whatever the mechanisms, the Wiretap Report indicates that, in contradiction to the predictions of a decade ago, encryption in wiretapped communications is simply not a problem for law enforcement.

What Sways the Courts?

Citizens and legislators alike have generally accepted police claims of wiretapping's indispensability as a crime-fighting tool but have felt a sense of disquiet about the ease with which it lends itself to invasion of privacy and political spying. As a result, Congress gave with one hand and took away with the other, allowing wiretapping but hedging it about with stiff warrant requirements and a strict reporting regime.

It is impossible to be sure what determines a guilty verdict. It is pos-

sible to ask jurors why they voted as they did but it is not clear that the jurors really know. Indeed, getting inside the mind of a jury is notoriously difficult. In trials with high-priced attorneys, a lot of time and energy is spent developing jury profiles. Much of this effort is guesswork.

The exacting standards for issuing wiretap warrants make it difficult to judge whether wiretaps were actually needed in the cases in which they have been used. The fact that we know of no definitive evidence for the value of wiretaps may mean that we are ignorant, that no one has ever tried to develop such evidence, or that there is none.

Transactional Information

The Digital Telephony Proposal came along when electronic surveillance was on the rise. Title III phone wiretaps were up from approximately 620 per year in the late 1980s to an average of 870 five years later.[26] In 1987 some 1600 pen registers had been installed; by 1993 the annual number was 3400. In 1987 the FBI, the Drug Enforcement Agency, the Immigration and Naturalization Service, and the US Marshals Service requested a total of 91 trap-and-trace devices; in 1993, the number was over 2000.[27] Part of the reason for this expansion in obtaining transactional information undoubtedly lies in improvements in telephone signaling that have made the information easier to obtain.[28]

As we noted earlier, transactional information cuts both ways. As in the case of the World Trade Center bombing, it can be useful in determining the structure of a conspiracy. It can also be used to forage into people's private affairs. Probes of Hillary Clinton's involvement in the Whitewater affair included reconstructions of how the first lady spent the days immediately after Vincent Foster's death.[29] Long-distance phone records were also used to expand the FBI's investigation of CISPES.

Constraints on Wiretapping

Title III requires that there be a court order before a wiretap can be installed.[30] In contrast with what is done when examining bank records or phone logs, a law-enforcement investigator who wants to wiretap has to draw up an affidavit showing that there is probable cause to believe that the targeted communication device—whether a phone, a fax machine, or

a computer—is being used to facilitate a crime. The crime must be serious and indictable. At the federal level, a wiretap request must be signed by a member of the Department of Justice at least at the level of Deputy Assistant Attorney General. Applications are decided upon by a federal District Court judge. Taps are approved for at most 30 days; extensions require a new court order.

The law obliges agents to tap only what is relevant to the investigation. This is called *minimization* and it requires an investigator to stop listening if the suspects are discussing issues not related to a potential crime, then turn it on several minutes later to check if the conversation has returned to indictable actions. The expense of having investigators do this provides a practical limit on the use of wiretaps. For example, in the Illwind investigation of Pentagon fraud, which ultimately tapped 26 telephone lines, several hundred agents were needed just for monitoring (Pasztor 1995, p. 190).

Criminals, whether they be defense consultants, drug dealers, or anyone else involved in a complex business, speak cryptically, and wiretapped lines reveal only part of the puzzle. In a recent FBI case, a wiretap picked up a conversation in which a murder plot was being discussed. The agents could not understand the street slang and jargon employed by the criminals and were unable to prevent the crime (Dam and Lin 1996, p. 89).

If the criminal evidence being sought is obtained before the end of the 30-day period, the law requires that the interception be terminated immediately. The raw numerical data provided by the *Wiretap Report* are insufficient to establish how carefully this rule is followed. In 1994, 22% of the wiretaps ran for the full authorization period but some wiretaps are terminated very quickly because there is a "pervasive pattern of innocence." In one case police discovered that one of their suspects had a very active telephone and moved to get a wiretap warrant. A brief period of monitoring revealed, however, that the calls were not evidence of an abundance of drug dealing but only of a popular teenage daughter.[31]

These restrictions, like others on wiretapping, are artificial. Though built into the law, they can be changed.[32] Indeed, one important restriction, minimization, has exceptions. For example, if the suspects are speaking a language not understood by the agent who is listening, tapes

can be made for later use when an agent who comprehends that language is available (Dam and Lin 1996, p. 400, note 17).

The FBI has consistently maintained that wiretapping is an expensive technique (Pasztor 1995, p. 186) and thus never likely to be put to broader use. An Australian-cabinet investigation of telecommunications interception, however, reached quite different conclusions, estimating the cost of a day's wiretapping as $Aus570, as compared to $Aus1376 for a listening device and $Aus2772 for vehicle tracking (Barrett 1994). Most of the cost of American wiretaps appears to due to the requirement that, in most cases, someone must monitor the tap in real time, turning a recorder on and off as the conversation drifts from innocent to incriminating and back.

The essential question about the future costs of wiretapping under US law is whether the courts will hold that minimization can be done by machines in a legally satisfactory way. Since electronic evidence gathered using search warrants is already handled in this way,[33] it seems possible that the answer will be yes. Should this occur, it would pave the way for much broader surveillance by law-enforcement agencies in the fashion currently practiced by intelligence agencies.

The FBI Makes a Case for Wiretapping

Beginning with the 1992 Digital Telephony Proposal, the FBI began a massive lobbying effort for passage of a wiretapping bill, presenting facts and figures that made a case for the importance of electronic communications to law-enforcement investigations. In the period 1985–1991, court-ordered taps conducted by the FBI reportedly figured in 7324 convictions, almost $300 million in fines levied, and over $750 million in recoveries, restitutions, and court-ordered forfeitures (FBI 1992a). Since the FBI conducts fewer than one-third of the non-FISA wiretap investigations, it can be assumed that the numbers above would be substantially higher if all such surveillance were taken into account. In 1992, during the presidency of George H. W. Bush, some White House staffers objected to the way the FBI calculated the losses due to organized crime, and disputed the FBI's claim that all 7324 convictions were due to elec-

tronic surveillance: "[S]ome [of these] convictions could probably still be obtained absent surveillance." (Anderson and Buchholz 1992) The Treasury Department observed: "It is difficult to do a critical analysis of DOJ's cost benefit package without a full explanation of how DOJ arrived at its cost/benefit figures, and what costs and benefits were included in those figures. It is not clear that DOJ knows, or could know, all the costs and benefits involved but this should be clearly stated." (Levy 1992) The vice-president's office also had trouble with the calculations, noting: "In several places in the analysis, figures are cited without reference to their sources or to how they were derived. For example, on p. 4 a figure of $1.8 billion is cited for potential economic loss. . . ." (McIntosh 1992) Despite the doubts cast upon these numbers, they appeared and reappeared in various briefings—most notably in 1993. Less than a month after President Bill Clinton took office, his senior director for intelligence programs received an FBI briefing paper on encryption, in which the FBI's questionable data were quoted (Sessions 1993b, p. 6).

The Digital Telephony Proposal Reappears

In 1994 the FBI prepared a revised Digital Telephony Proposal that limited wiretapping to common carriers and allocated $500 million to cover their costs. Carriers would have 3 years "after the publication by the Attorney General of a notice of capacity requirements"[34] to comply; after that, failure to fulfill a wiretap order could result in a fine of up to $10,000 a day. The revised proposal, the "Digital Telephony and Communications Privacy Improvements Act of 1994," was submitted to Congress in March 1994.

FBI Director Louis Freeh pressed for the passage of the new bill. Again the FBI claimed that the new technology was impeding its wiretapping ability. In a February 17, 1994, speech to the Executives' Club of Chicago, Freeh said: "Development of technology is moving so rapidly that several hundred court-authorized surveillances already have been prevented by new technological impediments with advanced communications equipment." In March, testifying before Congress, Freeh presented a lower estimate, citing a 1993 informal survey of federal, state, and local

law-enforcement agencies, which revealed 91 instances of recent court orders for electronic surveillance that could not be fully implemented (Freeh 1994b, p. 33). Even those numbers were not well substantiated.

Freeh's testimony had some curious gaps, the most serious of these was that, although Freeh was speaking in support of the Digital Telephony bill, his examples of electronic surveillance included electronic bugs.[35] Freeh himself seems confused about the distinction. When Senator Arlen Specter congratulated Freeh on the timeliness of his appearance (the FBI had just arrested Philadelphia mobster John Stanfa), Freeh readily agreed. The tape used in the case had come from an electronic bug.[36]

In April 1994, under an agreement that the details not be publicly released, Freeh supplied to the House and Senate Judiciary Subcommittees details of 183 instances in which the FBI had encountered difficulties in conducting court-authorized interceptions (USHR 103-827 *Telecommunications Carrier Assistance*, p. 14). The General Accounting Office, which earlier had complained about the FBI's lack of specificity in its electronic surveillance requirements, confirmed that the FBI did face technical problems in wiretapping as a result of the use of new digital technologies, including call forwarding, optical fiber, and ISDN (ibid., pp. 14–15). Despite Freeh's efforts, by late fall the Digital Telephony bill was in trouble. Freeh returned to Congress in a "last-ditch lobbying effort," pushing hard for passage of the bill that he had made his agency's highest priority (Chartrand 1994). His work paid off and the Digital Telephony bill became law under a new name: Communications Assistance for Law Enforcement Act (CALEA).[37]

CALEA put the government right in the middle of the process of designing telephone switches. It provided that, subject to federal appropriations to cover the costs of modification, telecommunications networks deployed after January 1, 1995 had to be configured to meet law-enforcement interception requirements,[38] whereas systems installed earlier did not have to be in compliance until the "equipment, facility, or service" was replaced or substantially upgraded (Communications Assistance for Law Enforcement Act, Public Law 103–414, §109). A cryptography provision was included in CALEA: "a telecommunications carrier shall not be responsible for decrypting, or ensuring the government's ability to decrypt ... unless the encryption was provided by the carrier and

the carrier has the information necessary to decrypt the communication" (ibid., §103(b3)). The law authorized the expenditure of $500 million to cover costs of the modifications. It also empowered the attorney general to determine the appropriate level of surveillance standards the telephone companies would have to meet. Attorney General Janet Reno decided that the FBI, the agency that had written and lobbied for CALEA, would be in charge of determining those very standards.

Within a year, the attorney general was to publish notice of the maximum capacity required by law enforcement. In October 1995 the FBI announced its analysis, for purposes of which the United States was divided into three parts on the basis of previous rates of telecommunications surveillance. In Category I (the area with the highest-density of communications interceptions, which presumably included the New York metropolitan area and Dade County, Florida[39]) the phone companies were to "expeditiously" increase the capacity for monitoring until 1% of the "engineered capacity" could be intercepted. (Interceptions might mean pen registers, trap-and-trace devices, or actual wiretaps.) In Category II areas these numbers were halved and in Category III areas the requirements for maximum surveillance were halved again. According to the FBI, "engineered capacity" is about 10% of the number of telephone lines, or some 15 million lines over the whole country.

These requirements translated to an extremely large number of simultaneous intercepts. There were approximately 160 million phone lines in the United States (FBI 1997b). Category I included about 12.5% of these, or a bit under 2 million lines; Category II was another 12.5% of the lines. Category III covered the remaining 75% of telephone lines. Thus the FBI requirements would result in capacity to wiretap approximately 30,000 lines simultaneously (EPIC 1995b). That is over 4 times the *annual* number of phone surveillances (total number of trap-and-trace devices, pen registers, and FISA and Title III wiretaps) in 1993 and 20 times the *annual* number of FISA and Title III wiretaps. Were the telephone carriers' engineered capacity to increase, so would law enforcement's ability to wiretap and track transactional activity.

A few months later there were complaints about other FBI interpretations of CALEA. The FBI proposed that the cellular telecommunications group adopt a standard enabling law-enforcement agencies to

determine the precise location of a wireless user within half a second (Markoff 1996). "In 1968 when they passed the original wiretap legislation, phones didn't move," said James Kallstrom.[40] "The notion that we in law enforcement should not be able to take advantage of the technology is a crazy notion (Markoff 1996)."

The industry objected. "The FBI is asking us to go beyond the legislation and ... turn all wireless phones into location beacons," fumed Ronald Nessen of the Cellular Telecommunications Industry Association (McGee 1996a). The legislators had been explicit on this very point: "... such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except as can be determined from the telephone number)" (CALEA, §103 a2B). In his congressional testimony, Louis Freeh had pledged that CALEA would not expand wiretapping powers.[41] In response to the industry objections, the FBI agreed to redraft its proposed cellular standards (McGee 1996a).

The FBI also reexamined the capacity issue. Scrutinizing surveillance activity county by county across the United States, in early 1997 the FBI proposed capacity numbers based on the maximum simultaneous surveillance that had occurred during the period from January 1993 to March 1995, defining "simultaneous surveillance" as surveillance that had occurred on the same day. Then the FBI added together all forms of telephone surveillance—wiretaps, penregisters, and trap-and-trace devices—to arrive at a baseline number. This was then multiplied by a growth factor to reflect the fact that the numbers were to apply in 1998.[42] The new regulations asked for the ability to conduct 39,767 "actual" simultaneous surveillances by 1998 and 57,749 "maximal" ones.[43] The latter number is 8 times the total electronic surveillances (wiretap, electronic, combination (USAO 1993), pen register, and trap-and-trace devices) conducted in 1993. Some of the increase arises as a simple consequence of the county-by-county approach—if a county had no surveillance activity during the time period, the FBI gave it a baseline of one (FBI 1997b)—but this inflation of the total figure may not affect Americans' privacy as much as other aspects of the FBI's capacity requirements.

The lines between wiretaps, pen registers, and trap-and-trace devices were blurred under the new proposals. The FBI's technique of combining the numbers for wiretaps, pen registers and trap-and-trace devices meant

that it was requesting the capability to perform 57,000 simultaneous surveillances, which could mean 57,000 uses of trap-and-trace devices or 57,000 wiretaps.

Freeh made several other efforts to increase the wiretapping capabilities of law enforcement. In 1995, immediately after the bombing of the Murrah Federal Office Building in Oklahoma City, Freeh proposed new legislation that would permit law-enforcement agents to obtain roving wiretaps (taps on a suspect who moves from phone to phone) without having to get individual court orders for each tap (Purdom 1995). Before the Oklahoma bombing, the FBI had paid little attention to right-wing militia groups and it is hard to imagine how expanded wiretapping capabilities could have prevented the act. Indeed, it was old-fashioned police work—including catching a speeder on a highway—that netted the suspects only a few days after the crime.

Responding to Oklahoma City, the White House sought expanded capabilities for electronic surveillance, including an expansion of Title III to cover *any* federal felony, the ability to use illegally obtained electronic surveillance information in court so long as the evidence had not been obtained in "bad faith," and the ability of the FBI to obtain long-distance telephone billing information without a court order. The White House also sought full funding for CALEA. Congress turned the president down on most of these requests; however, it approved funding for CALEA,[44] and it approved the use of subpoenas (as opposed to search warrants) to obtain local phone records.[45]

After the mysterious explosion of TWA Flight 800, in August 1996, Louis Freeh and James Kallstrom (in 1995 the latter became an FBI Assistant Director in Charge, New York Division) again urged an expansion of law enforcement's wiretap authority. President Clinton proposed that terrorist actions be included among the crimes for which electronic-surveillance orders could be obtained under Title III (terrorist actions were already included under FISA).[46] Clinton also recommended more liberal provisions for roving wiretaps, 48-hour emergency warrantless wiretapping, and profiling of airline passengers through electronic records (billing information and the like) to determine whose baggage should be the subject of careful searches for explosives.

The roving wiretaps were to be roughly akin to electronic writs of as-

sistance. Whereas the Title III required judicial approval of each wiretap placed on a suspect, the government now sought the ability to wiretap any telephone the suspect might be using—at a bar, a coffee shop, a gym, or a pizza parlor—without specific prior judicial approval of the wiretap's location. These proposals did not pass. The National Transportation Safety Board inquiry into the Flight 800 disaster, concluded that the explosion was the result of a spark in the fuel tank rather than terrorist action (NTSB).

The International Connection

In a behind-the-scenes effort, simultaneous with its domestic lobbying efforts for CALEA, the FBI worked the international front. Certain countries, including Britain, could be expected to be sympathetic to the FBI's viewpoint. In a worldwide context the British legal system appears similar to the American but there are sharp differences in the area of communications interception. There have, for example, been numerous charges of wiretaps on British labor unions and on the British "green movement"[47] and, in one instance, the private phone line of an Assistant Chief Constable who had initiated proceedings in the 'Industrial Tribunal' after failing to receive a promotion for which she had applied eight times (Donohue 2006, pp. 1166–1167).[48] The lack of a constitution and the British experience with terrorism (Irish terrorism has been a constant in England for at least a century) has led to a wiretap law which is less restrictive than the American one.[49]

The FBI briefed the international community on problems in communications interception at its research facility in Quantico, Virginia. Shortly afterward, the European Union (EU) opened discussions on interception.[50] The influence of the FBI was clear, although point 2 of the EU resolution lamely attempted to put some European control on the matter ("requirements of the member states will be conveyed . . . in order to avoid a discussion based solely on the requirements of the FBI").

A little over a year later, and without any public debate, the European Council passed a resolution on "realtime" monitoring capabilities. Like CALEA, the EU resolution required telecommunications providers to give law-enforcement bodies access to transactional data and call con-

tent. But the EU resolution went farther; it required providers of mobile services to give the locations of their subscribers.

The origins of the European initiative were clarified by a Memorandum of Understanding (MOU)[51] which extended the agreement to non-EU nations that chose to sign. Nations interested in participating were told to contact the General Secretary of the EU Council or the Director of the FBI for further information.

The EU's resolution and memorandum were not publicized. Although the resolution had the force of law on EU members, it was not brought before various parliamentary bodies. When, in the British House of Lords, the chairman of the Select Committee on European Affairs sought information on the resolution and the accompanying MOU, he was told that it was simply a "set of practical guidelines" and that it was not of parliamentary "significance."[52]

Standards bodies *were* kept informed, however. Service providers and manufacturers of telecommunications equipment were told that they would have to adhere to the standards of the resolution if they were to provide service or sell equipment to EU members or to signers of the MOU. In late 1996 the European Council began inviting non-EU members to participate in the MOU.[53] By early 1997 the FBI seemed to have made significant headway internationally in its attempt to develop law-enforcement access to telecommunications systems.

The FBI pressed for these surveillance technologies in a world where human rights guarantees are quite different from those of the United States. In the context of satellite-based communications systems, the European Union continued to look at surveillance issues. The EU Police Cooperation Working Group considered the possibility of "tagging" each subscriber "in view of a possibly necessary surveillance activity."[54] The United States may limit its use of wiretap surveillance to serious crimes and require a court order for such surveillance; however, as these excerpts from the US Department of State's Country Reports on Human Rights Practices for 1996 demonstrate, other countries do not.

- El Salvador: Wiretapping of telephone communications by the government is illegal, but occurs.

- Colombia: Despite a law, various state authorities monitor telephone conversations without obtaining authorization.
- Spain: Investigation continues into allegations of wiretapping by the National Intelligence Agency of private conversations between the king, various ministers, and other prominent figures.
- Greece: On occasion the government placed international and domestic human rights activists under surveillance.
- Angola: The government maintained a sophisticated security apparatus dedicated to surveillance, monitoring, and wiretapping of certain groups, including journalists, opposition leaders, and diplomats.
- Nigeria: Human rights and prodemocracy leaders reported that security agents regularly cut off or monitored their organizations' phones.
- Singapore: The authorities have the capability to monitor telephone and other private conversations. While there were no proven allegations that they did so in 1996, it is widely believed that the authorities routinely conducted surveillance on some opposition politicians and other critics of the government.
- China: All public dissent against party and government was effectively silenced. The 1982 constitution states that "freedom and privacy of correspondence of citizens are protected by law." In practice, however, authorities frequently record telephone conversations of foreign visitors, businessmen, diplomats, residents and journalists as well as Chinese dissidents and activists and others. Authorities also open and censor international mail.
- Indonesia: Security forces engaged in selective monitoring of local and international telephone calls without legal restraint. (USDoS 1997)

Hong Kong was an invited participant in these meetings from the beginning, despite the fact that in 1997 sovereignty of the British colony reverted to China, which has an abysmal record on human rights.

Encryption and Wiretapping

The ability to wiretap is substantially less useful if the conversations under surveillance are encrypted but the FBI sought to downplay CALEA's connections with encryption and, in particular, with escrowed encryption. After the introduction of the key-escrow program in 1993, many people raised questions about such connections. The government denied any ties between encryption and surveillance.[55]

Then in September of 1994, weeks before CALEA passed, FBI Director Freeh said otherwise. Asked how the FBI would respond should it encounter non-escrowed encrypted conversations in wiretapped communications, Freeh replied that he would go to Congress and ask for laws banning non-escrowed encryption.[56]

The White House disavowed the remarks, saying that Freeh tended to go his own way. In the following months, Freeh repeated his position, often quite strongly. (See e.g. Freeh 1996.) This did not surprise many of those who had opposed the original Digital Telephony Proposal. They had always expected such a response and that expectation was borne out by documents obtained by the Electronic Privacy Information Center through Freedom of Information Act litigation.

A 1991 NIST Public Key Status Report mentioned that the FBI was "working on draft legislation to control and license all cryptography" (USDoC 1991c). A memo written by National Security Advisor Brent Scowcroft on January 17, 1992 said that two days earlier the president had approved that the Department of Justice "should go ahead now to seek a legislative fix to the digital telephony problem, and all parties should prepare to follow through on the encryption problem in about a year." The Scowcroft memo continued: "Success with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix, and the encryption access options can be developed more thoroughly in the meantime."[57] (Scowcroft 1992)

CALEA passed in 1994. One half of the fix was now in, ready to be exploited for the encryption "problem."