Notes

Chapter 1: Introduction

1. (p. 4) The Watergate scandal, which forced the resignation of President Richard Nixon in 1974, was initiated by the installation of electronic surveillance in the Watergate offices of the Democratic National Committee. Watergate is only one of a number of cases in which electronic eavesdropping was used by the party in power for *political* purposes and was justified on grounds of "national security."

2. (p. 5) There is one major exception: radio and television are used to deliver a product to consumers.

3. (p. 6) At a 1995 talk in Brisbane, Australia, Ross Anderson of Cambridge University estimated the commercial market at over a billion dollars a year and likely to be augmented by another billion a year from developing industries (Anderson 1995), but the dollar figures do not appear in the printed paper.

4. (p. 7) The exact fraction is difficult to determine, partly because the budget is secret and partly because the most expensive items in the budget are spy satellites (some of which both listen to communications and take photographs).

5. (p. 10) This is one aspect in which telecommunications may forever remain less satisfactory than physical meetings.

Chapter 2: Cryptography

1. (p. 12) A signal sent by satellite can typically be received in an area thousands of miles across. One sent by microwave is hard to pick up more than a few miles from the "line of sight" between the towers. An intriguing approach to secure communication is used in some military satellite systems. Signals are transmitted from one satellite to another at frequencies that are absorbed by oxygen and cannot travel far enough through the Earth's atmosphere to be received on the

ground. This forces an eavesdropper to put up a satellite to spy on other satellites—an expensive proposition.

2. (p. 12) What it means to know someone in this sense is not straightforward. Essentially it means that your expectations about the person you are dealing with are correct. Those expectations may or may not include such identifying information as a name and address. There are some interactions, such as discussing your marital troubles with a stranger in a bar, in which what you are depending on is simply that the other party is, true to appearance, a sympathetic stranger who does not know your spouse and will not carry your tale back home.

3. (p. 13) The principle, alas, is often honored more in the breach than in the observance. For reasons discussed in chapter 3, there is a tradition of secrecy about cryptographic systems, both governmental and commercial. There is, however, a sense in which Kerckhoffs's principle holds, even in regard to secret systems. For example US government cryptographic systems that are used to protect TOP SECRET information are only classified SECRET and the equipment that embodies them is rarely classified higher than CONFIDENTIAL.

4. (p. 14) It is not made any clearer by the practice of using the terms "code" and "coding" for numerous transformations in modern computing and communication that have nothing to do with security.

5. (p. 15) You may also attempt to conceal the fact that what you are conveying is an encrypted message at all. This strategy—called steganography or covert communication—will be touched on from time to time in the text.

6. (p. 16) The police will recognize that they have a plausible candidate for a time-and-place message because the various positions in which only some digits are possible will all assume acceptable values.

7. (p. 17) A mask file is the digital input to a "fab line" that produces a computer chip. It can represent millions of dollars of engineering effort. Furthermore, semiconductors are often fabricated far from where they are designed and so, whether on a disk, by phone, or by Internet, the mask file must be transmitted from one to the other.

8. (p. 17) A one-part code is one in which the plaintext phrases and the code groups are simultaneously in alphabetical (or numerical) order so that the same book can be used for both encoding and decoding.

9. (p. 19) The Venona messages are available from the National Security Agency Web page: http://www.nsa.gov/venona/

10. (p. 21) The alphabets used in the first Vigenère table are in fact related. They were generated algorithmically by starting with a standard alphabet and using the GNU Emacs pseudo-random number generator to pick pairs of letters to be swapped. One thousand swaps were used to produce each alphabet. This process was intended only to produce such examples and is far from secure. The set

of alphabets given can probably be cryptanalyzed to find the parameters of the underlying pseudo-random number source.

11. (p. 21) The classical Caesar Cipher, in which every character is moved forward in the alphabet by three places, is the most famous example of a direct standard alphabet.

12. (p. 22) This form of CAVE is now used only in TDMA (Time Division Multiple Access) a legacy system still supported by Cingular but being phased out in favor of GSM and/or UMTS. (Source: private communication between Diffie and Greg Rose, September 2006).

13. (p. 24) This is usually called a *combiner* if it accepts several bits as inputs and produces one output and an *S-box* if its output is more than one bit.

14. (p. 25) Primary credit for the design of Skipjack appears to go to Paul Timmel, although this has not been officially confirmed. A patent application covering the system remains under secrecy order, presumably because it covers additional ways of using the system that are not needed by the secure email system and remain secret. A study of the published aspects of the escrow protocols makes it clear that the chips needed to encrypt blocks of more than 64 bits in order to escrow the 80-bit key.

15. (p. 26) The vast number of keys was offered as an argument for the unbreakability of ciphers during the Renaissance (Kahn 1967, p. 145) and probably earlier. The more general modern theories, including the theory of *non-deterministic polynomial time* or *NP* computing, (Aho et al. 1974) are far more mathematical but little more satisfactory. More specialized analyses of the vulnerability of particular cryptosystems to particular analytic methods has been more satisfactory.

16. (p. 26) In fact the cryptanalyst must also know enough about the plaintext to be able to recognize it; otherwise a correct solution to the problem cannot be distinguished from an incorrect one.

17. (p. 27) Chosen plaintext can arise in the real world in several ways. Suppose for example that the US Department of State delivers a diplomatique communiqué to a foreign embassy. The embassy must transmit the message home to its own government and is therefore likely to encrypt a message whose contents are known to the US government. Chosen plaintext may also be available to an organization that shares an encrypted channel—for example, a high-bandwidth satellite channel encrypted by the provider—with another organization.

18. (p. 27) This is popularly known as Moore's Law, and has held for the past several decades.

19. (p. 27) This doesn't work the other way around, because a large part of the cost of a computer is in such housekeeping aspects as its case and power supply, whose costs change less quickly.

20. (p. 28) In the US a typical TOP SECRET document is downgraded to UNCLASSIFIED in between 20 and 30 years.

21. (p. 29) Double DES allows a 112-bit key and appears at first to be adequate, but it is subject to an attack called "meet-in-the-middle." First discussed by David Snow at a National Bureau of Standards meeting in September 1976, this attack exploits a matching plaintext-and-ciphertext pair by encrypting the plaintext under all possible keys, decrypting the ciphertext under all possible keys, sorting the results, and looking for a match. Refinements of this technique are applicable in a surprising number of cryptanalytic circumstances.

22. (p. 29) The lifetimes of public-key cryptosystems are harder to quantify because terms such as RSA and Diffie-Hellman denote general techniques; they do not fix key lengths or register sizes.

23. (p. 29) For example, various forms of the German Enigma system were in use from the 1920s until well after World War II and some are probably in use today.

24. (p. 31) Rijndael and AES are not strictly speaking identical. The former includes modes for encrypting larger block sizes that are not part of AES.

25. (p. 31) The name Rijndael, which is pronounced "Rhine Dhal," is a combination of the names of its two designers: Joan Daeman and Vincent Rijmen.

26. (p. 33) As the name suggests, material under two-person control is never handled by one person alone. It would thus require a conspiracy of two people to, for example, make an unauthorized copy. Two-person control is supported by such things as safes with two combinations and areas called *no lone zones* in which at least two people must be present if anyone is present at all. "COMSEC" is short for "communications security."

27. (p. 33) Some keys used in the STU-III secure telephone, for example, have editions. Unless understood in the context of codebooks, the terminology seems peculiar for keys that never exist in any form other than an electronic one.

28. (p. 34) The term usually used for the system about to be described is *key distribution center* (KDC). Because more modern systems do not always distribute keys, the more general term KMF has come into use; we will use it throughout.

29. (p. 34) In fact, sharing a key with the KMF defines membership in the network.

30. (p. 35) The STU-II, an obsolete US military secure phone system was said to suffer from KDC congestion at busy times of the day.

31. (p. 38) Celebrated examples of this are to be found in the cases of Boyce and Lee (Lindsey 1979) and Whitworth (Blum 1987, pp. 280–326). In both cases, keys were saved rather than destroyed after use and were later sold to Soviet intelligence officers.

32. (p. 39) This technique of signing, which might be called a *primitive digital signature* has the disadvantage that in order to maintain the evidence of authorship, the recipient must store the ciphertext and must therefore either store the plaintext as well or decrypt the ciphertext again each time the plaintext is needed. In practice, what is done is to generate a *message digest* using one of several

message-digest algorithms (Schneier 1996, pp. 435–455) and compute a primitive digital signature of that.

33. (p. 40) It would be more accurate to call this *key agreement*. Unfortunately, the original name was generally accepted before it was observed that the things exchanged were not keys.

34. (p. 41) In the STU-II telephone system, calls to the KDC were initially too short to trigger billing and the contact had to be lengthened to accommodate telephone company complaints. (source: private conversation between Diffie and Howard Rosenblum circa 1980.)

35. (p. 41) This problem also bedeviled the STU-II. It is the problem solved by Rosenblum's invention of the two-part certificate (Rosenblum 1980).

36. (p. 42) It is possible but difficult to change network protocols. The current version, described here, is IPv4, which has 32-bit (sixteen billion) addresses. In a world with six billion people this no longer seems a generous allotment. A change is underway to IPv6 with 128-bit addresses but has yet to take off.

37. (p. 43) Although the protocol was adopted and published, development continues.

38. (p. 45) This is a codeword of obscure origin, not an acronym.

39. (p. 47) A lawsuit between General Motors and Volkswagen illustrates how valuable information about manufacturing design can be (Meredith 1997).

40. (p. 47) Consider, for example, the 1987 testimony of Cheryl Helsing, chairman of the Data Security Committee for the American Bankers Association, before Congress, "[I]f I were in charge of the Social Security system and concerned about getting those checks out every month, I would be much more concerned about whether those checks were in the correct amounts, made out to the right people, and that they did get out on time, than I would be concerned about an intruder gaining unauthorized access and looking at the files."

41. (p. 47) For example, all transactions over ten thousand dollars must be reported to the Internal Revenue Service. In *United States v. Miller* (425 US 435, 1976, p. 442), the Supreme Court ruled that deposit information does not have an "expectation of privacy" and may be subpoenaed. (A search warrant requires a higher standard of proof.)

42. (p. 47) A Citicorp electronic banking system used directly by corporate customers for funds transfer was penetrated. Posing as a corporate customer, a user from St. Petersburg, Russia, transferred funds to an account in Finland; the money was withdrawn from the bank the next day. The falsified transaction was accomplished with a personal computer and the phone lines. Over the next several months, this scenario was repeated, with the user's locale changing to Rotterdam, San Francisco, St. Petersburg, and Tel Aviv. Citicorp became aware of the thefts after several customers complained of irregularities in their accounts. By August, $12 million had actually been moved, and $400,000 had been stolen.

Relative to the amount that Citicorp transfers daily (about $500 billion) this is relatively little, but of course banks' business is providing security, and in that sense the theft loomed large. Access to the system required a customer's authorization code; it is believed that the perpetrator (allegedly one Vladimir Levin) had an accomplice within the system who supplied these. The bank has now changed its security to using one-time passwords (Carley 1995; Hansell 1995).

43. (p. 48) An Alaskan oil company investigated why it had been losing leasing bids by small amounts to a competitor and discovered that a line between a computer in its Alaska office and one at its home base in Texas were being wiretapped. A competitor was intercepting pricing advice being sent from the Texas office (Parker 1983, p. 322).

44. (p. 48) The most notable of these is the Digital Millennium Copyright Act, Public Law No. 105-304, 112 Stat. 2860.

45. (p. 49) *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, National Counterintelligence Center, Washington, D.C., July 1995, as reported in (Dam and Lin 1996, p. 33).

46. (p. 49) Command 9438, para 10, as cited in Fitzgerald and Leopold 1987, p. 148.

47. (p. 50) This directive was issued after a laptop containing information on 26.5 million US veterans and their families was stolen from a VA analyst's home. The data had not been encrypted.

48. (p. 53) One example occurred in the 1970s, when thousands of phone conversations between IBM executives conducted on the company's private microwave network were systematically eavesdropped on by Soviet intelligence agents. NSA informed IBM of the eavesdropping (Landau et al. 1994, p. 1). A similar incident occurred in the 1980s with a different US corporation (Dam and Lin 1996, p. 68).

49. (p. 54) Electronic commerce is still a loosely defined term. At present, examples range from individuals purchasing physical objects over the Internet by sending electronic mail to businesses making automatic purchases from their suppliers using Electronic Data Interchange protocols. The grand conception of large-scale purchase and sale of information over the network using a combination of digital credit cards (which would sign digital sales slips with digital signatures) and electronic cash (which would be anonymous and have many of the properties of physical money) has yet to materialize but electronic commerce using ordinary credit cards and web pages is thriving.

50. (p. 55) Email, which traditionally was done via a user's machine, now can be done through a website; gmail or Yahoo are examples of such a service. This is part of the "Web 2.0" experience.

51. (p. 56) Zfone (Zimmerman 2006) is an add-on security mechanism that can

be used with any Voice over IP system, created by Philip Zimmerman, the author of PGP.

Chapter 3: Cryptography and Public Policy

1. (p. 57) "Probabilistic cryptography," as put forth by Goldwasser and Micali (1984), is a formalization of the long-standing method of using *message indicators* to guarantee that a cryptosystem starts each message in a unique state.

2. (p. 60) For quite some time, communications security was poor in parts of the US government (particularly the Department of State) that lacked access to the services of the military cryptographers.

3. (p. 61) A 2400-bit-per-second mode of operation is one of the *Minimum Essential Requirements* of the third generation secure telephone unit (STU-III), which went into use in 1987.

4. (p. 63) There appear to have been rotor-based voice systems, but these were probably analog scramblers that filtered the signal into several bands employed rotors to shuffle the bands in a constantly changing pattern.

5. (p. 64) A small number of serious books were published in Europe, in particular Eyraud 1959.

6. (p. 64) Papers on points pure of mathematics whose cryptographic inspiration is clearly visible to people familiar with the subject were written by Andrew Gleason, Marshall Hall, W. H. Mills, and presumably others.

7. (p. 64) Kennedy's orders do not mention cryptography, but require that US nuclear weapons be put under *positive control* of the National Command Authority (the President *and* the Secretary of Defense), wherever in the world they may be located. What this came down to was that they could not be armed by anyone unable to send them properly encrypted messages. The key component in this program is the *permissive action link*, which, in effect, issues an encrypted order to a nuclear weapon. Earlier PALs used conventional cryptography; more recent ones use public-key techniques.

8. (p. 65) Source: private conversations between Diffie and Feistel.

9. (p. 65) Eventually, in the late 1960s, the cryptographic system Feistel's group designed was bundled together with the existing modes of operation of the Mark X IFF. The result was called the Mark XII (there never was an XI), and its cryptographic mode was Mode 4. The Mark XII is employed extensively by the military aircraft of the US and its allies.

10. (p. 65) Source: private conversations between Diffie and Carl Engelman of Mitre in the 1970s and between Diffie and Horst Feistel circa 1990.

11. (p. 66) The importance of the Federal Information Processing Standards is illustrated by FIPS 1, the American Standard Code for Information Interchange

or ASCII. The government's adoption of this code, which is ubiquitous today, made it dominant over the rival EBCDIC encoding used by IBM, then the world's largest computer manufacturer.

12. (p. 67) The one in the 2984 is now called the Alternate Encryption Technique. At least two other IBM systems were also called Lucifer. One designed by John Lynn Smith, but never developed into a product, presents the fullest exposition of Feistel's techniques (Smith 1971). Another system called Lucifer was used only as a tutorial device (Feistel 1973).

13. (p. 67) At NSA, Howard Rosenblum, Deputy Director for Communication Security, and Doug Hogan; at NBS, Ruth Davis, Seymour Jeffery, and Dennis Branstad.

14. (p. 67) NOFORN means "No foreign dissemination allowed." This is an odd designation for many NSA algorithms, since several of the most important are NATO standards.

15. (p. 68) In testimony to congress, NSA Director Bobby Ray Inman asserted that public key cryptography had been discovered at NSA 10 years earlier. It appears that Inman preferred to give credit to three Brits with clearances than three Yanks without. The work in question is that of GCHQ employees—James Ellis, Clifford Cocks, and Malcolm Williamson—and was carried out between late 1969 and mid 1976. The precise scope of the British discoveries did not emerge until after James Ellis's death in the fall of 1997, when Ellis's retrospective history of the work and at least some of the original papers were released (CESG). Although GCHQ claimed priority and most of the discoveries it did make (apparently neither digital signatures nor knapsack systems had occurred to them) were earlier than those made in the public world, the two efforts overlap. Ellis's paper in 1969 is several years before any of the outside work but Williamson's secret internal memo on "Diffie-Hellman" comes two months after the idea had been presented at the US National Computer Conference.

16. (p. 69) The term is a misnomer because the items exchanged are not actually keys. In contemporary literature, the more precise terms *key negotiation* or *key agreement* are preferred, but the original terminology persists.

17. (p. 70) In the early 1970s, for example, secrecy orders were placed on some of the inventions of Horst Feistel, nucleus of the cryptographic research group at IBM.

18. (p. 70) Secrecy orders are often helpful to a company because they delay the granting (and thus expiration) of its patents until a time when the invention is more appropriate to the market. In 1939 the famous actress Hedy Lamarr filed for the first patent on frequency hopping radio (Markey 1942). Had this application been kept secret until the 1970s, when spread spectrum technology emerged from military into civilian applications, Hedy Lamarr would have enjoyed a much more comfortable retirement.

19. (p. 72) Uriel Feige, Amos Fiat, and Adi Shamir had discovered a practical im-

plementation of "Zero-Knowledge" protocols (Feige et al. 1987). They submitted a US patent application even as Shamir lectured worldwide on the algorithm. The Army requested a secrecy order be placed on the invention. This was classic shut-the-barn-door-after-the-horse-has-fled; for several months the researchers had been giving lectures about the work. Since secrecy orders forbade the discussion of the research with the foreign nationals, and Feige, Fiat, and Shamir were all Israeli citizens, what American law could do in this situation was unclear. Fearing to present the work at an American research conference under the circumstances, Shamir let various colleagues know about the problem. Help came. Shamir's lawyer got an anonymous call from Dr. Richard A. Leibler, retired head of R5, telling him precisely whom to call to get the secrecy order lifted. Shamir publicly thanked "the NSA . . . who were extremely helpful behind the scenes . . ." (Landau 1988, p. 12)

20. (p. 72) It was rumored that DES was used by the Argentines in the Falklands War and had seriously hampered British SIGINT.

21. (p. 72) CCEP was modeled on the earlier Industrial Tempest Program, begun in the 1970s, which encouraged industry to build electromagnetically shielded versions of their products.

22. (p. 72) The government also appeared to be laying legal framework for broadened availability of cryptographic equipment. For as long as anyone could remember, all cryptographic devices approved for protection of classified traffic had been owned by the government. Now with NSA's COMSEC Instruction 6002 it provided two ways that government contractors could own the equipment and charge the costs back to government contracts in the same way they did with buildings, computers, or safes.

23. (p. 73) Type I equipment is managed through COMSEC accounts and is basically available only to organizations with government contracts. Under the new rules, owners of Type II equipment would not have COMSEC accounts but would need to have the equipment supplied to them by government sponsors. From the point of view of the user, the distinction between having a government sponsor and having a government agency as customer was minor.

24. (p. 74) Development of the STU-III was paid for directly by NSA, beginning by funding five competitors to prepare proposals.

25. (p. 74) Only a year late, and about 50% over the target price.

26. (p. 74) The Type II version, affected by the same fluctuation of availability rules as other Type II equipment, was not a success. In a move incomprehensible to marketing people everywhere, the Type II STU-III, though advertised from the beginning as inferior to the Type I, was always priced higher. This is at least partly because the Type II never achieved the volume of production originally planned and did not benefit from the same economy of scale as the Type I.

27. (p. 74) Perhaps to help NSA avoid the need to pay royalties for public key technology, just as it used secrecy to avoid paying Hebern.

28. (p. 74) "This policy assigns to the heads of Federal Government Departments and Agencies the responsibility to determine what information is sensitive, but unclassified and to provide systems protection of such information which is electronically communicated, transferred, processed, or stored on telecommunications and automated information systems." (Poindexter 1986, p. 542)

29. (p. 76) Ten years later, DES remains a Federal Information Processing Standard.

30. (p. 76) By this time Poindexter was deep in the middle of the Iran-Contra controversy, and the administration was loath to have him appear at any congressional hearing lest the questioning veer to Iran-Contra. Thus Poindexter did not appear when first requested, and the House committee then subpoenaed him (USHH *Hearings on HR 145*, p. 381). A discussion ensued between the White House and the committee, and the committee delayed hearings an additional two weeks, while the White House withdrew Poindexter's directive (Carlucci 1987), hoping to avoid Poindexter's appearance in Congress.

The committee insisted that the former Presidential National Security Advisor appear, which he did, accompanied by counsel. Despite the fact that Representative Jack Brooks, chair of the Committee, promised that questions would be limited to issues related to the NSDD-145 and the Poindexter Directive (USHH *Hearings on HR 145*, p. 399), Poindexter declined to answer any questions and pleaded the Fifth Amendment. The congressmen, having achieved the withdrawal of the Poindexter directive, did not pursue the matter further.

31. (p. 76) "The development of standards requires interaction with many segments of our society, i.e. government agencies, computer and communications industry, international organizations, etc. [NIST] has performed this kind of activity very well over the last 22 years. NSA, on the other hand, is unfamiliar with it." (USHR 100-153 *Computer Security Act*, p. 26)

32. (p. 77) The Committee on Governmental Operations was the subject of a similar attempt by NSA. "In January 1981, the Director of the NSA even went so far as to write this Committee and complain that the Committee had not forwarded to NSA a copy of its investigative report, 'The Government's Classification of Private Ideas,' *prior* to its issuance. As pointed out by Chairman Brooks in reply to NSA, Congress does not submit its reports to Executive Branch agencies for prereview." (USHR 100-153 *Computer Security Act*, pp. 21–22)

33. (p. 78) The Budget Office also noted that the Act would result in savings due to the elimination of fraud and other financial losses (USHR 100-153 *Computer Security Act*, p. 43).

34. (p. 78) Officially known as the Balanced Budget and Emergency Deficit Act of 1985, the act set annual deficit targets for five years, aiming for a balanced budget in 1991. It was never fully implemented.

35. (p. 78) There was an additional $800,000 of 'reimbursable' funds from other agencies; such funds are typically for help in deploying advanced technologies.

36. (p. 79) One example of such deference to NSA was NBS's failure to support its own standard in the International Standards Organization. About 1985 ISO took up consideration of DES as an international standard and approached the American National Standards Institute, which in turn approached its cryptographic committee X3T1, on which NBS sat. NBS cast its vote in X3T1 against recommending DES; ANSI abstained in the international committee, and ultimately ISO did not adopt DES. Another example is Raymond Kammer's decision that NIST would support NSA's decision that NIST abandon RSA as a choice for a public-key signature standard (Source: private conversation between Landau and Kammer, December 19, 1996.)

37. (p. 80) Source: private conversation between Landau and McNulty, December 2, 1996.

38. (p. 81) Source: private conversation between Landau and McNulty, December 2, 1996.

39. (p. 81) Schnorr applied through the EEC for a patent, thus obtaining patents in Germany, United Kingdom, France, the Netherlands, Italy, Spain, Belgium, Switzerland, Sweden, Liechtenstein, and Austria; see Schnorr 1989, Schnorr 1990, and Schnorr 1991.

40. (p. 81) NIST countered this last point by noting that the Kravitz algorithm was roughly 25 times faster than the RSA algorithm in signing (USDoC 1991a).

For most applications speed of verification is more important than speed of signing, since a signature is signed only once and may be verified many times. In some applications such as signing software to protect against the introduction of viruses, the signature may literally be checked billions of times over the lifetime of the product. On the other hand, there is something to be said for making the signing operation more economical, because it is the one that uses the secret information and is best done in an isolated environment like a smart card. At the time, such cards had limited computational power.

41. (p. 82) "The key question during the hearings was: Should a military intelligence agency, NSA, or a civilian agency, [NIST], be in charge of the government's computer standards program?" (USHR 100-153 *Computer Security Act*, p. 19)

42. (p. 82) "Observers—including OTA—consider that [the MOU] appears to cede to NSA much more authority than the act itself had granted or envisioned, especially considering the House report accompanying the legislation." (USC-OTA 1994, pp. 13–14)

The General Accounting Office said: "[T]his Memorandum of Understanding made NSA appear to more influential in NIST's standard-setting procedure relative to cryptographic systems than was intended by the Congress in the Computer Security Act of 1987." (USGAO 1993a, p. 16)

43. (p. 83) Claus Schnorr's patent was licensed from him by RSA Data Security, which provides DSS code in its cryptographic toolkits. On the other hand, many

people have studied Schnorr's patent and maintain that it does not cover DSS. To date the issue of the patent's validity has yet to be litigated.

44. (p. 83) Source: private conversation between Landau and Brooks, January, 17, 1997.

45. (p. 83) Source: private conversation between Landau and Kammer, December 19, 1996.

46. (p. 84) Source: private conversation between Landau and Kallstrom, January 16, 1997.

47. (p. 84) New York City's District Attorney of the fifties, Frank Hogan, was a strong proponent of wiretapping, and in 1955 he testified to Congress: "In these and in many other important prosecutions, the investigative technique of wiretapping was invaluable. In a substantial number I may say, gentlemen, it is indispensable." (USHH 84 *Wiretapping*, p. 322)

48. (p. 84) There were 419 electronic surveillances conducted in New York in 1994 (AO 1995, pp. A26–A33, and p. A90) (AO 1996, pp. 54–60 and pp. 126–140).

49. (p. 84) There were 53 court-ordered surveillances in California during 1994 (AO 1995, pp. A2–A7 and p. A8), (AO 1996, pp. 34–38 and p. 94).

50. (p. 84) Source: private conversation between Landau and Kallstrom, January 16, 1997.

51. (p. 85) Source: private conversation between Landau and Brooks, January 17, 1997.

Chapter 4: National Security

1. (p. 88) On October 24, 1969, President Nixon announced a decision to make narcotics a matter of foreign policy. The CIA was asked to "contribute to the maximum extent possible in the collection of foreign intelligence related to traffic in opium and heroin" (USDoJ 1976, pp. 46–47). President Ford later called the smuggling of opium to the United States a "national-security" issue (ibid., p. 59).

2. (p. 88) In a speech in the Spring of 1997, President Bill Clinton invoked the name of national security in support of education.

3. (p. 88) Cryptography, once so central to information security as to be almost indistinguishable from it is now reduced to the status of one important part.

4. (p. 89) The CIA Foreign Broadcast Information Service publishes transcripts of numerous foreign radio shows.

5. (p. 89) A similar inference might simply have been drawn from looking at the number of cars in the parking lot or the number of lighted windows. The significance of the pizza story lies in showing how difficult operations intelligence

is to counter. Security officers may well have thought to hold meetings in inner offices, or to take measures to avoid having the parking lot look full. Any large scale operation, however, leaves many telltale traces and it is hard to anticipate and cover up all of them. Keeping the kitchens open all night might stem the flow of pizza orders only to create other signs of activity: the amount of raw food being ordered, the quantity of garbage put out for collection, or the hours of the kitchen staff. In many organizations where all professional staff members are required to have security clearances, employees such as cooks, whose activities can be confined to daytime hours and a small part of the building, are not.

6. (p. 89) An amusing example of the CIA's aggressive interest in using travelers as spies is given by the Hemingway scholar Michael Reynolds. In 1975, Reynolds made persistent attempts to get a visa to Cuba in order to study Hemingway's library. In the process, the CIA contacted him on the chance that if he got to Cuba, he might get to meet Fidel Castro—who was known for surprise visits with tourists. Reynolds also gives plausible evidence that the CIA's enthusiasm for his trip to Cuba went so far that they had his phone bugged (Source: Michael S. Reynolds, *Hemingway's Reading*, 1910–1940, Princeton University Press, 1981.)

7. (p. 90) Another new, and very controversial, form of intelligence is: RUMINT, intelligence gathered from unreliable sources, including rumors. Many in the intelligence community discount the value of such intelligence, and, indeed, blame RUMINT for the faulty intelligence the United States used prior to the 2003 war in Iraq (Kristof).

8. (p. 91) These, however, have created embarrassments of their own. Consider the shooting down of an American U2 spy plane over the Soviet Union in 1960 or the capture of the American spy ship *Pueblo* by North Korea in early 1968.

9. (p. 92) This appears to have been a longer-range, and higher-altitude version of the mechanism that seagulls use to detect an impending storm and fly inland. It is an eerie commentary on the success of secrecy in the intelligence community that this project, which is supposed to have been abandoned, was kept secret for nearly 50 years. In 1995 it was offered as the explanation for the Roswell Incident of 1947, which is, despite official denials, believed by many people to have been the crash of an alien spaceship (Thomas 1995).

10. (p. 92) Distinguishing nuclear explosions from other events, such as large lightning bolts or explosions of meteors in the atmosphere, is not easy. The satellite reacts less to the total energy of the blast than to the form of the flash. Nuclear explosions have a characteristic two-humped flash caused by gamma ray induced formation of nitrogen pentoxide (N_2O_5). The time between the humps is called the *bhang metre* and is characteristic of the type of weapon.

11. (p. 93) For example, the Krasnoyarsk radar, which was alleged by the US to violate the ABM treaty, was photographed from space only after its location had been reported by a human source (Richelson 1987, p. 79).

12. (p. 93) The study of radar signals sometimes involves elaborate provocations

designed to create the impression that an attack is in progress and thereby to fool an enemy into using radars that are not meant to "come to life" except under battle conditions. A persistent theory of the strange movements of Korean Airlines 007, which led to its being shot down, is that its purpose was to provoke the radars of the Kamchatka Peninsula air defense system into action so that other aircraft—RC-135's designated Cobra Ball—could observe them (Johnson 1978).

13. (p. 94) It has long been known that, unless a radio is specifically designed to conceal the information, one can discover what station is being received by measuring the frequency of the local oscillator. This, however, depends on knowing the intermediate frequency, and that information may not be available about a radio of unknown type. Around 1960, it was discovered that many radios had a frequency shift in the local oscillator, resulting from an effect of the automatic gain control on the high-voltage supply, that was proportional to the frequency of the received signal. That discovery portended vastly expanded exploitation of unintentional signals emitted by receivers (Wright 1987, p. 93).

14. (p. 94) One function of the US Argos satellites was to monitor telemetry from Soviet missile tests. This fact is believed to have come to Soviet attention as a result of the activities of Christopher Boyce, who was subsequently convicted of spying on CIA projects at a contractor, TRW, in Southern California (Lindsey 1979).

15. (p. 94) In order to prevent tampering with the satellite, control link transmissions are often encrypted. The device used for this purpose by the military, the KI-23, is the main product of Mykotronx, later known as the maker of Clipper and Capstone chips.

16. (p. 95) In the 1950s, British counterintelligence employed a corps of "watchers" to follow hostile diplomats. The watchers communicated with MI5 by radio, and in an attempt to conceal the their activities, they tried communicating in code. Peter Wright recalls in his autobiography *Spycatcher* that this was of little use; the mere occurrence of the traffic was sufficient to reveal to the Russians where the watchers were operating (Wright 1987, pp. 52–53). In a much more recent example of the same phenomenon, Tsutomu Shimomura (Shimomura 1996, Shimomura 1997, p. 76) reports that in tracking Kevin Mitnick, who had broken into Shimomura's computer, Mitnick's use of cryptography "didn't slow them down at all." Quite a different example came to light in conjunction with the Yom Kippur war of 1973: it was said that the Israelis should have been alerted that something was up by the improved communication security on the part of the Egyptians.

17. (p. 95) A remarkable example of this occurred shortly before the Normandy invasion in World War II. The Japanese military attache in Germany demanded a tour of German defenses in Normandy and reported what he had seen to Tokyo. That transmission, presumably encrypted in Purple, was read by the Allies and

supplied them with an expert assessment of German channel defenses (Kahn 1967, p. 508; Boyd 1993). Another example is provided by the Gamma Guppy intercepts of the early 1960s, in which the US embassy in Moscow monitored mobile phone traffic from the limousines of Soviet officials (Bamford 1982, p. 283).

18. (p. 95) Physical taps on lines do have a role, however, and not just in counterintelligence work. In the 1980s a former NSA employee named Ronald Pelton was recruited by the Soviets. One of the things he allegedly told them was that the United States had placed a tap on a cable running under the Sea of Okhatsk. According to a Soviet publication, the tap, which weighed 12 tons, was powered by plutonium and serviced by US submarines.

19. (p. 96) The largest Soviet intercept station outside the USSR was at Lourdes, Cuba. It could pick up satellite transmissions intended for receivers in Washington, New York, and other eastern cities.

20. (p. 96) In the 1970s and the 1980s, there was a war of words between US and Soviet diplomats over Soviet microwave interception activities from a residence the Soviets maintained at Glen Cove, New York (Broad 1982).

21. (p. 98) On the face of it, this incident, in which the Israelis attacked and nearly sank the *Liberty*, is inexplicable. It was claimed that the *Liberty* should actually have been hundreds of miles away, in the waters off Cyprus, but that its orders got delayed. If the *Liberty* was, as publicly claimed, spying on the Arabs, there is no reason for the Israelis to have attacked it. On the other hand, the Israelis' claim that they mistook the *Liberty* for an Egyptian freighter hardly seems credible. Loftus and Aarons (1994) have produced an explanation that, although not supported by overwhelming evidence, is at least sensible. It is their thesis that the *Liberty* was actually listening to traffic from Israeli tanks and manpack radios as part of a secret deal to report weaknesses in the Israeli southern front to Egypt. To do this, it would have to have been quite close.

22. (p. 100) VoIP, with its superb adaptation to mobility, presents related and even more serious difficulties. It is fairly easy to intercept VoIP in a way that gets some part of some of the calls but comprehensive coverage is quite hard.

23. (p. 100) During the shootdown of KAL 007 in September 1983, for example, signals intelligence was severely hampered by the fact that only the transmissions of the interceptor pilots and not those of their ground controllers could be intercepted (Hersh 1986, p. 70).

24. (p. 100) Multiplexing takes three common forms. Two of these are well illustrated by broadcast radio. *Frequency division multiplexing* is the phenomenon by which different stations have different frequencies. To select a station you tune to its frequency. *Time division multiplexing* is the phenomenon that distinguishes programs. Within the frequency of a given station, you listen at a particular time to find the right program. The third form is called *code division multiplexing*. Code division multiplexing is one of the benefits of *spread spectrum communi-*

cation, in which a transmitter uses a wide range of frequencies, often by hopping rapidly from one to another. Using code division multiplexing, multiple transmitters can avoid interference with little prior coordination. The more advanced cordless telephones are perhaps the most common items that use code division multiplexing.

25. (p. 102) The cryptanalysis of World War II systems is discussed in detail in Deavours and Kruh 1985 and in Welchman 1982. Cryptanalysis of classical systems makes up much of the content of *Cryptologia*, the journal of cryptographic history. Cryptanalysis of contemporary cryptosystems can be found in the *Journal of Cryptology* and in the proceedings of numerous annual and biannual conferences, such as Crypto (held in late August in Santa Barbara, California), Eurocrypt (held at a different location in Europe each spring), and Asiacrypt (held each year in the Asia Pacific region). A particularly noteworthy book on the subject is Biham and Shamir 1993. Particularly noteworthy books include the ones by Biham and Shamir (Biham and Shamir 1993) and the encyclopedic reference work by Menezes, van Oorschot, and Vanstone (Menezes) which includes some cryptanalytic material. Sample chapters of the latter are available at: http://www.cacr.math.uwaterloo.ca/hac/ (last viewed 29 August 2006).

26. (p. 102) Most books on the breaking of the German Enigma cryptosystem during World War II focus on the researchers, especially Alan Turing, at Bletchley Park. The actual reading of most of the traffic, however, was done with several hundred special purpose computing machines, called *bombes*, which were operated 24 hours a day by women from the Women's Reserve Navy Service (Welchman 1982, pp. 138–148).

27. (p. 102) Many systems in use today still have either 40-bit keys (which can be searched easily) or 56-bit keys (which can be searched with some difficulty). *Dragging key* (looking through all possible keys) thus has a role to play in contemporary cryptanalysis. A far more subtle, but also universal, cryptanalytic method is the Berlekamp-Massey algorithm (Berlekamp 1968; Massey 1969). It is a fact that any sequence of bits (keystream) whatsoever can be generated by a linear shift register of sufficient length. The Berlekamp-Massey algorithm automatically produces the right register. A major design criterion in modern cryptography is that the "right register" be too long for this approach to be practical.

28. (p. 102) Traffic analysis is fundamentally a matter of discovering the relationships among a number of "address spaces," some observable and others inferred. The call signs, like phone numbers, are the name space of the communications network. Direction finding, emitter identification, and collateral intelligence allow these to be correlated with physical positions, individual pieces of equipment, or command functions.

29. (p. 103) Sanitization goes hand in hand with the desire of intelligence officers to keep raw intelligence out of the hands of their customers. The British learned

this lesson in a particularly blunt fashion at the Battle of Jutland in World War I. Before the battle, a British officer of the line walked into the intelligence center and asked the location of the radio callsign of the admiral commanding the German fleet. He was told, correctly, that it was located in the Jade River. What the officer actually wanted to know was the location of the admiral, who had switched call signs when the fleet had set sail precisely in order to fool the British about his location. British intelligence was not fooled; it knew the German admiral's new location and new callsign. Nonetheless, as a result of the intelligence center's releasing raw intelligence on call-signs, rather than finished intelligence on the locations of forces, the Germans achieved their purpose. The British fleet delayed sailing and the battle, which might have been a major British victory, was indecisive (Beesley 1977).

30. (p. 104) In 1961, William Martin and Bernan Mitchell, two NSA cryptanalysts, defected to Moscow and gave a press conference in which they revealed interception by the US of its allies' communications. According to David Kahn, the loss of intelligence was felt immediately (Kahn 1967, p. 694).

31. (p. 104) In the mid 1970s a panel headed by Nelson Rockefeller concluded that the Soviets were intercepting conversations on microwave telephone channels from Capitol Hill. Even though congressmen are not supposed to discuss classified information over unsecured telephones, the information intercepted from such high-level people, particularly when taken in aggregate, has tremendous intelligence potential. It has been speculated that the Soviet activity was detected because the volume of traffic intercepted was sufficient to permit correlations between fluctuation in the Capitol Hill traffic and communications from the Soviet Embassy to Moscow to be observed.

32. (p. 104) Bobby Inman remarked in an informal discussion after his talk at AFCEA West in Anaheim, California on January 8, 1981 that NSA's product had never been better.

33. (p. 105) Speaking in 1980 at the IEEE Wescon conference in San Francisco, Robert Morris (then at Bell Labs and later Chief Scientist of the National Computer Security Center) said: "We are just leaving a period of relative sanity in cryptography that began shortly after the First World War. During that time people spoke of cryptosystems that were secure for hours, days, weeks, months, and sometimes, years. Before it and after it, they spoke of cryptosystems that were unbreakable."

34. (p. 105) In the 1980s, for example, NSA built two new operations buildings, a new research and engineering building, a chip fabrication facility, and two advanced laboratories away from Fort Meade to be operated by a contractor. Major construction at Fort Meade has subsided since that period but GCHQ, its British cognate, has built a giant round building (called "the doughnut") in Cheltenham.

35. (p. 105) Kim Philby is believed to have had access to information on the

Venona program; the Soviets would thus have learned about it soon after it began.

36. (p. 106) This laboratory is the subject of Aleksandr Solzhenitsyn's novel *The First Circle* (1968) and of a later memoir by Lev Kopelev (who was Rubin in the novel). It is Kopelev (1983, pp. 52–55) who discusses the remarkable technique of assessing the security of *mosaic* or *two-dimensional* (time and frequency) voice scramblers they were developing by printing out a sonogram (a plot of energy and frequency over time) and measuring the time it took to solve the sonogram as though it were a jigsaw puzzle and reassemble it into one representing human voice. In *The First Circle*, which takes place around Christmas 1948, Solzhenitsyn and his fellow workers are under the gun from Stalin to deliver "secret telephony" within about six months. The year I read it was 1974. That year, digitized speech (pre-requisite to high-quality secret telephony or as we call it "secure voice") was the main topic at the ARPA (Advanced Research Projects Agency) Principal Investigators' Conference.—WD

37. (p. 106) After the end of the Cold War Soviet crypto machines began to appear in the collector's market. One of these is a 10-rotor machine called Fialka. Since 'fialka' is a Russian word (meaning violet) and 'Albatross' is a western codeword, the names are of no help in establishing a relationship. Fialka, however, had a number of models spanning the appropriate period. It is interesting to note that although Fialka has the same number of rotors as Sigaba, its rotors are all in one row, compared with Sigaba's two.

38. (p. 108) In the 1980s, US companies were not permitted to export optical-fiber communications systems to the USSR, presumably on the ground that communications carried by fiber would replace radio communications and could not be intercepted.

39. (p. 108) The raw data rate of the V.fast standard is 28 kilobits-per-second, but it incorporates real-time data compression and can often achieve effective throughput of 200 kbps—far more that is available on many current leased line networks.

40. (p. 109) The difficulty of separating the two signals in the communication of autocancelling modems is a function of the size of the *constellation*, the number of combinations of amplitude and phase used in communication. V26ter uses four points, V32bis uses 32 and the more recent V.fast uses 64.

41. (p. 109) Much of dynamic routing technology was developed for another purpose: it increases the survivability of networks against direct attack, a phenomenon that occurs primarily, though not entirely, during open hostilities.

42. (p. 110) AT&T developed a specialized cryptographic device for protecting signaling channels (Myers 1979; Brickell and Simmons 1983, pp. 4–5).

43. (p. 110) The US government's successor to the STU-III, the Secure Terminal Equipment (STE), is primarily an ISDN phone, but is compatible with STU-III. The STE is being manufactured by Lockheed Martin and systematically being

used to replace the aging STU-IIIs. Likewise, the British Brent telephone is an ISDN instrument.

44. (p. 111) Skype can operate between Internet-connected devices or between such devices and more conventional phones. In the latter case, the conventional telephony portion will not be covered by Skype encryption.

45. (p. 111) A precise figure is made difficult to obtain by the problem of deciding what counts as encrypted. At one time, most of the world's encrypted traffic consisted of scrambled pay-tv broadcasts, a good example of the sort of encrypted traffic that either does not interest intelligence agencies or can be accessed without resorting to cryptanalysis.

46. (p. 112) The bombing of communication facilities in France forced the Germans to use radio for their communications with Berlin. The traffic that thereby became available for interception was encrypted with the Siemens and Halske T52 cipher machine. This was especially fortunate because the principles of operation of the T52 are similar to those of the Lorenz SZ40 (an online cipher machine that had earlier been used with radios), and cryptanalytic methods developed to attack the SZ40 proved applicable to the T52. It was to attack these machines, not the Enigma, that the Colossus—arguably the first computer—was built.

47. (p. 112) Photographs of the destruction of a bridge in Baghdad were repeatedly shown during the early days of the attack. The bridge was destroyed, not for its capacity to carry cars and trucks, but to destroy the optical fiber that ran underneath.

48. (p. 113) One development has been the *HARM* or *High-Speed Antiradiation Missile* which is launched from aircraft to home in on the fire-control radars of anti-aircraft weapons and destroy them.

49. (p. 113) The destructive effects of the *Electromagnetic Pulse* or *EMP* was first observed by the United States in a high altitude nuclear test above Johnson Island in the South Pacific. The test damaged electronic equipment as far away as Hawaii. The technique, which has since been refined and can be produced by non-nuclear means, goes under the name *High Energy Microwave* (Van Keuren 1991; Schwartau 1994; AWST 1997a).

50. (p. 113) Jamming describes transmissions intended to interfere with an opponent's communications or other signals such as radar. This is not always a wartime phenomenon. In the mid-eighties HBO was briefly pushed off the air by a more powerful beam carrying a message critical of HBO activities.

51. (p. 113) Communications deceptions are classified as *imitative* if they mimic the communications of an opponent. More subtle communications deceptions are *manipulative*: they do not misrepresent the allegiance of the sender, but convey a false impression of its activities. In the months leading up to the invasion of Normandy in 1944, General George Patton commanded a division, stationed

in southern England, that was pretending—by its communications and other activities—to be an entire army.

52. (p. 114) The distinction between viruses and worms (which might better have been called bacteria) is biologically based. Biological viruses are combinations of genetic material with protective protein coats. They function by invading the genetic material of cells and instructing the cell to produce more viruses. In a similar way, computer viruses incorporate themselves into computer programs. When the program is executed, the virus is executed and exploits the occasion to copy itself into other available programs. A worm, by comparison, is a "free-living" program that invades a computer or a network and tricks its host into running it as a separate process.

53. (p. 114) Viruses first became visible in the 1980s. Their origin is unclear. (I recall discussing the notion of viruses—though not what term was used—with my colleague Jack Holloway in 1970. When I mentioned this to Oliver Selfridge, member of the Baker committee and a longtime advisor to NSA, he told me that the notion had been about in the late 1950s.—WD)

54. (p. 114) Although the claim that viruses were employed against the Iraqis in the first Gulf War appears to be groundless, there are repeated discussions of their development for military applications (AWST 1993; Richardson 1991; Robinson 1993b).

55. (p. 115) A cut out of this sort that prevents the tracing of phone calls is called a *cheese box*.

56. (p. 115) This was at the Air Force IT Conference in Montgomery, Alabama (Onley).

57. (p. 117) Even introducing a small number of errors makes the analysis of data far more difficult, and an error rate of just over 11% reduces the information content of a channel by half. In the mid-1980s, the notion of having the DoD give out false information about weapons developments was publicly mooted (North 1986).

58. (p. 118) Motorola manufactured a device called Ladner to encrypt analog telephone lines. Linkabit, California Microwave, Racal Datacom, and Cylink made high-speed DES-based encryptors to protect the digital ones.

59. (p. 118) AT&T developed DES and public-key-based encryption devices that were subsequently applied to securing common channel interoffice signaling (Myers 1979).

60. (p. 121) As we will see later, this is no longer entirely true.

61. (p. 122) People often refer to high grade cryptographic systems as being "unexportable." In fact, much of the best US cryptographic equipment—for example, the KG-84, general purpose data encryptor—is sold to the governments of NATO countries and other American allies and in some cases even "co-manufactured" in foreign countries. Exports of equipment of this sort are gov-

erned by individually approved export licenses and usually take place under the *Foreign Military Sales Program*.

62. (p. 122) Precisely what the capabilities of intercept equipment are is hard to tell. Under a deal between NSA and the Software Publisher's Association, some cryptographic systems with 40-bit keys could be rather freely exported by the early 1990's, when embodied in "mass market software." Since computers could already execute 2^{40} instructions in an hour at that time, 40-bit keys did not represent very much security from a commercial viewpoint. On the other hand, it is unlikely that intercept devices, which are comparable in price to high-end workstations, could do any better. Since decisions about intercept must be made not in hours, but in fractions of a second, it is prudent to presume that NSA knew how to break the ciphers in question with a workfactor substantially less than 2^{40}.

63. (p. 123) That the true mission of NSA's export-control office is intelligence and not administration is revealed by its organizational designation: G033 (later changed to Z033) rather than Q or D—arguably a failure of operational security.

64. (p. 123) Aside from electronic funds transfers between banks, businesses use telecommunications for a variety of other high value communications. Oil companies routinely prospect at locations scattered around the world. Their analyses of core samples and other data form the basis for bids on drilling rights. Bids by multinational corporations on contracts distant from their headquarters require communication of information that is sometimes valuable enough to affect the company's survival. Internal transfers of equipment and supplies, can rival actual funds transfers in value.

Chapter 5: Law Enforcement

1. (p. 126) Fingerprints serve two related but distinct functions in police work: identifying available people uniquely and identifying unavailable people via *latent* fingerprints on objects at crime scenes. The former function was not new—fingerprints impressed in clay had been used by the Babylonians for identification of written tablets—but before fingerprinting Europeans used the Bertillion system of body measurements. Fingerprints were an improvement both in being more precise and in having a forensic as well as identificational function (Kelling 1991, p. 960).

2. (p. 128) Earlier *stipendiary police*, like bounty hunters and some sheriffs, were paid at least in part through a share of collected fines—a mechanism whose corrupting potential is obvious. In some measure this system has been reintroduced via forfeiture laws that reward police departments, thought not their members directly, with a share of the proceeds derived from selling property confiscated from criminals.

3. (p. 128) The British scholar Sydney Fowler Wright (1929), commented that so

great was the influence of the police over the magistrates' courts that they had come popularly to be called "police courts."

4. (p. 128) The police commonly express the sentiment "We don't make the laws, we merely enforce them." Although it is technically true that laws are made by legislatures, the law-enforcement community exercises substantial influence over the process. Not only do senior law-enforcement officials ranging from the assistant directors of the FBI to the attorney general frequently testify before Congress on pending bills; many bills are first seen by Congress and its staff in the form of drafts prepared by law-enforcement agencies.

5. (p. 130) Even circumspect statements on a wiretapped phone can be quite useful. Fat Ange Ruggerio of the Gambino crime family was not aware his phone was being wiretapped when he told a colleague, "[I'm handling some] H." The FBI was listening, and agents photographed Ruggerio as he made deliveries to three different drug traffickers (Blum 1993, p. 83).

6. (p. 130) Gravano read the government transcripts. He saw the strength of the Federal case and learned that Gotti was angry with him for being too greedy (Blum 1993, pp. 255–257 and pp. 317–318). Fearing that Gotti was developing a strategy to blame him for various crimes, the underboss turned the tables, and testified against Gotti (Blum 1993, pp. 319–326).

7. (p. 130) Although US agents learned of meetings, they never succeeded in tracking Ames to one (Weiner et al. 1995, pp. 229–230, pp. 245–246).

8. (p. 131) A tap of this kind is often called a bug and not clearly distinguished from a microphone listening to the room. Such devices are inexpensive and easy to install. A radio bug built into an RJ11 "octopus plug" has been advertised in *Popular Electronics* by a company called Seymore-Radix. Its price is about $30.

9. (p. 131) For a more detailed exploration of the ways a line can be tapped see Dash et al. 1959 and Fitzgerald and Leopold 1987.

10. (p. 131) On his first visit to Democratic National Committee Headquarters in the Watergate Building, James McCord succeeded in placing a bug in the phone of the chair's secretary. But this elicited very little useful information, so McCord returned a few weeks later for a second—and fateful—try.

11. (p. 133) Apparently because the results were written down with a pen.

12. (p. 133) In Europe this has not been the case. Long-distance bills were instead compiled by means of a tone-based message-unit system that did not reveal the called number.

13. (p. 133) Signaling System 7 (SS7), introduced to support ISDN in the 1980s, passes the identity of the called phone from switch to switch throughout the whole length of the call.

14. (p. 133) Clifford Stoll (1989, p. 68) gives a dramatic account of such an exercise that took place as late as the mid 1980s.

15. (p. 133) Privacy blocking will prevent the ID information from being given to

the receiving telephone but will not conceal it from either a telephone company switch or private branch exchange attached to the network by a DS1 connection.

16. (p. 133) Analysis of billing information during their investigation of the 1993 bombing of the World Trade Center led the FBI from the initial suspect to his co-conspirators (Mashberg 1993; Bernstein 1994). More recently, it has come to light that after the 9/11 attacks the National Security Agency began receiving billing information in vast quantities for similar purposes.

17. (p. 135) In the United States and Canada, 911 is the phone number for emergency services: police, fire, and ambulance.

18. (p. 135) Another conspirator in the 1993 World Trade Center bombing, Eyad Ismoil, was picked up through a matching of telephone records with airline manifests; he was later convicted (McKinley 1995a).

19. (p. 135) Investigators also used photos from several days before the explosion to prove that Timothy McVeigh was the "Robert D. Kling" who, on the afternoon of April 17, 1995, in Junction City, Kansas, rented the Ryder truck used in the bombing. Days and weeks after the bombing investigators meticulously reconstructed McVeigh's movements on April 17. Surveillance photos taken at a McDonald's about a mile from the Ryder agency showed McVeigh at the restaurant at 3:49 and 3:57 PM on that day. Shortly afterward, "Kling" rented the truck. When prosecutors claimed that the McDonald's photo was of McVeigh, his lawyer did not dispute the point. The photo was taken several days before there was any hint it would be useful in a criminal case—and *then the evidence was available when needed* (Brooke 1997a).

20. (p. 136) For decades, state-issued drivers' licenses have been *de facto* identity cards in the US. Congress has until recently rejected the introduction of national identity cards. Now it has changed its mind in a remarkably oblique manner. As the *New York Times* put it, "What Congress [did] instead is to ram through a bill that turns state-issued driver's licenses into a kind of phony national identity card through the mislabeled 'Real ID' provision. And in order to make absolutely sure there's no genuine debate, the sponsors have tied it to a crucial bill providing funds for American troops in Iraq and Afghanistan" (New York Times 2005). (The Real ID Act was introduced as HR 418, but was eventually attached to the emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief 2005 (HR 1268).) The Real ID Act required that beginning in 2008, state drivers licenses were to adhere to common machine-readability standards determined by DHS. The licenses were to include name, birth date, sex, ID number, a digital photograph, address—and the data had to be verified with the federal government and other states before a driver's license could be issued. No longer would drivers be allowed to have more than one license, which had been a common practice, for "snowbirds" who spent their winters in Florida and their summers in northern climes, and only citizens and legal residents would be permitted to have such licenses.

21. (p. 137) The provisions were later extended to the other armed forces.

22. (p. 138) Other investigators have reached different conclusions (Burnham 1996, p. 218).

Chapter 6: Privacy: Protections and Threats

1. (p. 142) Article 17 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks (United Nations 1985, p. 149).

2. (p. 143) In East Germany clergymen and other religious workers were informants; siblings informed on one another, and there were even husbands who informed on their wives (Kinzer 1992).

3. (p. 143) The main purpose of the Privacy Act of 1974 (Public Law 93-579) was to ensure that federal records on individuals were accurate, timely, complete, and relevant (US-PPSC 1977, p. 17).

4. (p. 145) The term "Secretary of State" must have designated an office more like that of the secretary of state of California (whose duties include certifying election returns) than like that of the US secretary of state, whose position in Britain is called "foreign secretary."

5. (p. 145) "You will know from whom this comes without a signature: the omission of which as rendered almost by the curiosity of the post office. Indeed a period is now approaching during which I shall discontinue writing letters as much as possible, knowing every snare will be used to get hold of what may be perverted in the eyes of the public." (Thomas Jefferson, in a letter to James Thomas Callender, October 6, 1799; see Jefferson, *Works*, Federal Edition, Vol. 9, p. 488).

6. (p. 145) From one post office per forty-three thousand inhabitants in 1790, the US postal system had grown to one post office per slightly over one thousand in 1840 (Ellis, p. 51). "There is an astonishing circulation of letters and newspapers among these savage woods," wrote Alexis de Tocqueville in 1831 (deTocqueville, p. 283).

7. (p. 145) The complaints centered on theft rather than lack of confidentiality.

8. (p. 146) Mail from prisoners of war, and between the Union and the Confederacy, was a different matter; it was routinely opened and censored (Scheele 1970, p. 88).

9. (p. 146) Wiretapping appears to have been rare.

10. (p. 147) See, e.g., *State v. Litchfield* 58 Me. 267 (1870), *National Bank v. National Bank* 7 W. Va. 544 (1874), *United States v. Babcock* 3 Dill 567 (1880), *United States v. Hunter* 15 Fed. 712 (1882), *Ex Parte Jaynes* 70 Cal. 638 (1886),

Re Storrer 63 Fed. 564 (1894), *Western Union Telegraph Co. v. Bierhaus* 8 Ind. App. 563 (1894), as reported in (Seipp 1977, p. 59).

11. (p. 148) In fact, people felt more secure than was justified. Confidence in the sanctity of first class mail was so great that most people were unaware that there were legal circumstances under which it could be opened.

12. (p. 150) Under the Fourteenth Amendment the citizens are protected from intrusions by the states.

13. (p. 152) Specifically, the court held that, "Where, as here, the Government uses a device that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion, the surveillance is a Fourth Amendment 'search,' and is presumptively unreasonable without a warrant." (Kyllo, p. 38).

14. (p. 153) Bork was a candidate for the Supreme Court. During his confirmation hearings, the press reported his video-rental habits, which tended to run to Hitchcock and Cary Grant.

15. (p. 154) For example, the Social Security Administration matches its Supplemental Security Income Benefit with the Internal Revenue Service's tax data so as to avoid paying duplicate benefits (USGAO 1990, p. 24)

16. (p. 154) PL 93-579.

17. (p. 154) Under the Privacy Act, there continue to be notices in the Federal Register about federal systems of records, so it is theoretically possible to gather the aggregate information. In practice, such counts are likely to be inaccurate.

18. (p. 155) In 1900 there were about two-billion people and no database of two-billion items. Today many people could store the names of the world's six-billion people on the multi-hundred gigabyte disks of their laptops and laptops will surely have the capacity to store full dossiers on everyone long before a database of such dossiers is collected.

19. (p. 156) Thus, for example, the doings of the Mississippi Sovereignty Commission, in which, the state, from 1956 to 1977, authorized spying, harassment and intimidation of civil-rights workers in order to delay or halt desegregation, only became public in 1998 (Kettle 1998).

20. (p. 156) Act of June 18, 1929, ch. 28, sec., 11, 46 Stat. 25.

21. (p. 157) Thomas Clark, who later became US Attorney General, was assigned to the Western Command. He recalled that a Census Bureau member had shown him files detailing exactly where Japanese-Americans lived (reported in (Okamura 1981, pp. 112–113)).

22. (p. 157) Postal workers are permitted to open first-class mail, but only with the explicit permission of the addressee or if the employee is trying to determine an address to which to send the mail (39 U.S.C. 3623(d)). Otherwise, a warrant is needed; that has been US law since at least 1878 (*Ex Parte Jackson*, 96 US 727, 1878, p. 733).

23. (p. 158) See Chapter 2 of Charns 1992, for a fuller discussion of this incident.

24. (p. 159) "Evidence indicates that the FBI did not believe that the Communist Party [constituted] as serious a threat as it had in the 1940s" (USSR 94 *Intelligence Activities: Rights of Americans*, p. 66).

25. (p. 159) These are from the following FBI memos: Memo from FBI Headquarters to New York Field Office, July 11, 1960; Memo from FBI Headquarters to New York Field Office, December 16, 1960; Memo from FBI headquarters to New York Field Office, November 3, 1961, as reported in (USSR 94 *Intelligence Activities: Staff Reports*, pp. 363–364).

26. (p. 159) $42,500 for disruption activities by the FBI, $96,500 for surreptitious entries by the FBI, and $125,000 for the FBI's use of informants (*Socialist Workers Party v. Attorney General of the United States*, 73 Civ. 3160, 1986).

27. (p. 161) The justification was "Martin Luther King, Jr., head of the Southern Christian Leadership Conference (SCLC), an organization set up to promote integration which we are investigating to determine the extent of Communist Party (CP) influence on King and the SCLC, plans to attend and possibly may indulge in a hunger fast as a means of protest." (Sullivan 1964)

28. (p. 161) The memo is reproduced on p. 713 of USSH 94 *Intelligence Activities: Huston Plan*.

29. (p. 161) In a letter from the FBI to Vice President Agnew, Ralph Abernathy, President of the SCLC, is characterized as a man "who, although he advocates nonviolence, has invited violence by some of his statements." (USSH 94 *Intelligence Activities: FBI*, p. 494, Exhibit 38-3.) In 1970 the FBI forwarded information on Abernathy's private life to Vice President Agnew. The Church Committee hearing exhibits include a letter the FBI [signature blanked out] to the Vice President, "... In response to your request, there is attached information regarding ... Ralph David Abernathy ... The material also includes information about [his private life] (sic) ..." Exhibit 38-3, in (USSH 94 *Intelligence Activities: FBI*, p. 494).

30. (p. 162) Bond, a Georgia state legislator, and Jackson, executive director of SCLC Operation Breadbasket, were active in the civil rights movement. Baez and Guthrie (son of the legendary Woody Guthrie) were folk singers, Coffin, chaplain at Yale, Spock, a physician and the author of the well-known *Baby and Child Care*, that had been the bible of American parents in the post-war years, were all active in the anti-war movement. Stevenson made it into the files because of his association with Jackson (O'Brien 1971, p. 127). Mikva, a member of the House active in the anti-war movement, said that he learned from Senator John Tunney "how I became eligible for the files. Jesse Jackson is a constituent of mine; Adlai Stevenson is a friend of mine; and my wife used to work for the American Civil Liberties Union." (Mikva 1971, p. 130). Ralph Stein, formerly with US Army, Counterintelligence, in (Stein 1971, p. 266) told of the surveillance of Baez, Bond, Coffin, Guthrie, Jackson, King, and Spock. Stein did not mention

Mikva or Stevenson, but Mikva testified to the existence of Army surveillance files on both, as did O'Brien. (Mikva 1971, p. 136; O'Brien 1971, p. 120 and p. 127)

31. (p. 163) This included Lloyd Norman, a *Newsweek* reporter writing on US military plans in Germany, and Hanson Baldwin, a *New York Times* reporter and military historian who had written on Soviet missile sites (USSR 94 *Intelligence Activities: Rights of Americans*, p. 63).

32. (p. 163) During Johnson's administration Attorney General Nicholas deB. Katzenbach had wrested control of electronic surveillance back from the FBI and imposed certain limitations on its use (USSR 94 *Intelligence Activities: Rights of Americans*, p. 105).

33. (p. 163) As he signed the bill, Johnson said: "Title III of this legislation deals with wiretapping and eavesdropping.
My views on this subject are clear. In a special message to Congress in 1967 and again this year, I called—in the Right to Privacy Act—for an end to the bugging and snooping that invade the privacy of citizens.
I urged that the Congress outlaw 'all wiretapping and electronic eavesdropping, public and private, wherever and whenever it occurs.' The only exceptions would be those instances where 'the security of the Nation itself was at stake—and then only under the strictest safeguards.'
In the bill I sign today, Congress has moved part of the way by

— banning all wiretapping and eavesdropping by private parties;

— prohibiting the sale and distribution of 'listening-in' devices in interstate commerce.

But the Congress, in my judgement, has taken an unwise and potentially dangerous step by sanctioning eavesdropping and wiretapping by Federal, State, and local law officials in an almost unlimited variety of situations.
If we are very careful and cautious in our planning, these legislative provisions could result in producing a nation of snoopers bending through the keyholes of the homes and offices of America, spying on our neighbors. No conversation in the sanctity of the bedroom or relayed over a copper telephone wire would be free of eavesdropping by those who say they want to ferret out crime." [Johnson 1968]

34. (p. 164) Attorney General Edward Levi later wrote Kraft that the FBI's file "did not indicate that [Kraft's] activities posed any risk to the national interest" (Pincus 1976).

35. (p. 165) "This demonstration could possibly attract the largest number of demonstrators ever to assemble in Washington, D.C. The large number is cause for major concern should violence of any type break out. It is necessary for this Bureau to keep abreast of events as they occur, and we feel in this instance ad-

vance knowledge of plans … would be most advantageous to our coverage and the safety of individuals and property." (Hoover 1969b)

36. (p. 165) These included Columbia University's Mathematics and Science Library, the New York Public Library, the Lockwood Memorial Library at the State University of New York at Buffalo, the Courant Institute of Mathematical Sciences Library, the University of Maryland at College Park Engineering and Physical Sciences Library, the University of Houston Library, and the Engineering and Mathematical Sciences Library at the University of California at Los Angeles (Foerstal 1991, pp. 54–69).

37. (p. 166) The Foreign Agents Registration Ac (22 U.S.C. 611 et. seq.) was passed in 1938 in response to Nazi propagandists working to influence the US government and the public. The law requires those in pay of a foreign government seeking to sway US public opinion through engaging in political activities, acting in a public relations role, soliciting or distributing items of value for a foreign principal, or representing the foreign principal to a member of the US government to register with the Foreign Agent Registration Unit within the Criminal Division of the US Department of Justice.

38. (p. 168) Two of the eight, Khader Hamide and Michael Shehadeh, were permanent residents and thus were charged with being associated with a group that advocated destruction of property, a deportable offense for non-citizens; the others were charged with "technical" violations of their visas (ibid., p. 35).

39. (p. 168) One member of the case was finally granted his petition for citizenship in 2006 (Caldwell).

40. (p. 168) The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Public Law 107-56); see chapter 11 for a discussion of the Act.

41. (p. 168) See chapter 5 for a discussion of the Real ID Act.

42. (p. 169) Despite repeated warnings from the General Accounting Office, these browsings continued. There were 449 unauthorized file searches in 1994, 774 in 1995, 797 in 1996 (USGAO 1997; Richardson 1997).

43. (p. 169) During the investigation of the "sugar lobby" in 1962, ten phone lines of a Washington law firm were wiretapped. Several advisors to Martin Luther King who were lawyers were wiretapped (USSR 94 *Intelligence Activities: Staff Reports*, p. 340).

Chapter 7: Wiretapping

1. (p. 173) "Eavesdrop" does not, as it might appear, mean to hang from the eaves and listen to what is going on in an adjacent room. The eavesdrop is the area within the eaves of a house, what we would today call, the footprint of the

house, and to eavesdrop is to trespass within the eavesdrop in order to look or listen.

2. (p. 175) In 1998 it was revealed that the Los Angeles Police Department had routinely used information gleaned from ongoing—and legal—wiretaps to open new investigations in which, in direct contravention of the law, suspects were never informed of the role that wiretaps had played in their case, even during trial (Krikorian 1998).

3. (p. 177) "General Stuart was always accompanied by his own telegraph operator, who had no difficulty in connecting his portable instrument at any point of the wires, and could thus read off and reply to the messages *in transitu*. One of these on the occasion in question, was addressed to the Quartermaster-General, who had just sent off to the Federal army a large number of mules, all of which had fallen into the hands of Stuart. Accordingly, the following message was despatched [sic] to this official :—"I am much satisfied with the transport of mules lately sent, which I have taken possession of, and ask you to send me soon a new supply.—J.E.B. Stuart."(von Borcke, p. 168).

4. (p. 182) Hoover went to extraordinary lengths to hide the wiretap logs as well as records that would reveal wiretapping had occurred; the FBI Director even hid the name of the filing system in which wiretap records were stored. After the Coplon case, wiretap information went into the "June" files, June being Hoover's codeword for "Top Secret." See Theoharis and Cox 1988, pp. 256–261 for a discussion of Hoover's methods.

5. (p. 184) For many years stories circulated that before Hoover's annual testimony to Congress the FBI Director had wiretaps removed, and then had the taps reinstated afterwards. This way Hoover could minimize the number of active wiretaps reported to Congress. The Church Committee carefully examined the number of wiretaps for the dates in question and concluded this story was apocryphal (USSR 94 *Intelligence Activities: Staff Reports*, p. 302).

6. (p. 185) He certainly had no objection to doing so when the president made such requests (FBI 1975a; USSR 94 *Intelligence Activities: Staff Reports*, p. 313–314).

7. (p. 185) The wiretapped justices include Hugo Black, Stanley Reed, William O. Douglas, Abe Fortas, and Potter Stewart (Charns 1992, pp. 17, 25, 87); (Hoover 1970).

8. (p. 194) The Judiciary Committee Report on the act said that "each offense was chosen because it was intrinsically serious or because it is characteristic of the operations of organized crime," (USSR 90-1097 *Omnibus Safe Streets and Crime Control*, p. 97) and that "the last provision [interstate transport of stolen goods] is included to make it possible to strike at organized crime fencing" (USSR 90-1097 *Omnibus Safe Streets and Crime Control*, p. 98).

9. (p. 194) In an emergency, a wiretap may be placed without a warrant; however, if a warrant is not obtained within 48 hours, the information produced

—like any electronic communication intercepted in violation of Title III—may not be received in evidence or even divulged (Omnibus Crime Control Act 1968 §515).

10. (p. 194) The fax and computer provisions were added by the Electronic Communications Privacy Act.

11. (p. 194) The stringent requirements for obtaining a wiretap order do not, however, mean that such surveillance may only be done as a "last resort." (*United States v. David Smith*. 893 F. 2nd 1573 (9th cir. 1990))

12. (p. 194) This requirement was codified in a supplementary law enacted in 1970 (Omnibus Crime Control and Safe Streets Act §2518(4)).

13. (p. 197) Aside from Morton Halperin, there were:

- National Security Council members Helmut Sonnenfeldt, Daniel Davidson, Richard Sneider, Winston Lord, and Tony Lake;
- State Department members Richard Pedersen and Richard Moose, Ambassador William Sullivan;
- Department of Defense member Colonel Robert Pursley;
- White House staff John Sears, William Safire, and James McLane, and;
- correspondents Henry Brandon (*London Sunday Times*), Hedrick Smith (*New York Times*), and Marvin Kalb (CBS News).

14. (p. 197) The *Post* began to publish the papers after the *Times* was served with an injunction barring publication.

15. (p. 198) Ellsberg had also been picked up on the Halperin wiretaps; during the 21 months, Ellsberg had been overheard on 15 occasions (Hersh 1983, p. 325). Halperin was circumspect in his conversation, but Ellsberg was not; he talked about taking "trips" and carrying "stuff" to a friend's house—clear allusions to drugs. The wiretap transcripts, including these comments, went to the White House.

When Ellsberg's role in leaking the Pentagon Papers was discovered, Kissinger, who had earlier hired Ellsberg as a consultant to the National Security Council, tried to distance himself from the leaker. He disparaged Ellsberg to the president by calling him a drug abuser. When Nixon queried Kissinger about this, the National Security Advisor replied "There is no doubt about it." (Hersh 1983, p. 384) Thus we see the insidiousness of wiretaps; the Halperin-Ellsberg wiretapped conversations, *which had never showed any evidence of national-security leaks* (ibid., p. 397), were forwarded to the White House, where the private discussions between two colleagues became ammunition for character assassination and worse.

16. (p. 202) The Church Committee observed that certain types of surveillance carried out by the intelligence agencies had been illegal at the time (USSR 94 *Intelligence Activities: Rights of Americans*, pp. 12–13). The members recommended

legislation to regulate "domestic security activities of the Federal Government" (ibid., p. 295).

17. (p. 202) *Recommendation 6.*—The CIA should not conduct electronic surveillance, unauthorized entry, or mail opening within the United States for any purpose (USSR 94 *Intelligence Activities: Rights of Americans*, p. 302).

18. (p. 202) *Recommendation 15.*—NSA should take all practicable measures consistent with its foreign intelligence mission to eliminate or minimize the interception, selection, and monitoring of communications of Americans from the foreign communications.

Recommendation 16.—NSA should not be permitted to select for monitoring any communication to, from, or about an American without his consent, except for the purpose of obtaining information about hostile foreign intelligence or terrorist activities, and then only if a warrant approving such monitoring is obtained in accordance with procedures similar to those contained in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (USSR 94 *Intelligence Activities: Rights of Americans*, p. 309).

19. (p. 202) *Recommendation 52.*—All non-consensual electronic surveillance should be conducted to judicial warrants issued under authority of Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

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

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

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

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

(d) Such electronic surveillance should be exempt from the disclosure requirements of Title III of the 1968 Act as to foreigners generally and as to Americans if they are involved in hostile foreign intelligence activity (except where disclosure is called for in connection with the defense in the case of criminal prosecution) (USSR 94 *Intelligence Activities: Rights of Americans*, pp. 327–328).

20. (p. 202) For the purposes of FISA, a "United States person" is a citizen, a permanent resident alien, a group of such people, or a US corporation.

21. (p. 202) There are two exceptions to this rule. After a declaration of war, the president, through the attorney general, can authorize a wiretap for foreign intelligence purposes for up to 15 days without a court order. A court order is

also unnecessary if communications are exclusively between foreign powers or involve intelligence other than spoken communications from a location under the exclusive control of a foreign power.

22. (p. 202) Originally there were seven judges on the FISA Court, but the USA PATRIOT Act increased the number to eleven.

23. (p. 203) An approved application may result in several wiretap orders, since the target may be using several communication devices.

Chapter 8: Communications in the 1990s

1. (p. 205) This was the best-case scenario; the worst-case showed no access to intercepted communications by 1995 (Advanced Telephony Unit 1992).

2. (p. 206) In 1994 the US Telephone Association estimated that the costs for call forwarding information alone would come to as much as $1.8 billion (Neel 1994b, p. 101). New equipment and software for wiretapping were estimated to be another $450 million (Neel 1994a, p. 60).

3. (p. 206) In particular, by 1991 virtually all mid-size and large companies were using PBXs, with more than 25 million lines (NTIA 1992).

4. (p. 207) "Everything considered, would you say that you approve or disapprove of wiretapping?" In 1994 76% of Americans said they disapprove (USDoJ 1994b, p. 173).

5. (p. 207) All the missing reports occurred in state electronic surveillance cases.

6. (p. 207) In the case of multiple crimes, the *Wiretap Report* lists only the most serious crime as the reason for the order.

7. (p. 207) Since a case takes several years to wend its way through the courts, convictions are usually reported several years later.

8. (p. 208) 355 F. Supp. 523, 542 (S.D. Calif. 1971), cited in Schwartz 1974, p. 194.

9. (p. 208) The case involved bid-rigging in the window-replacement industry. Lawyer Benjamin Brafman argued that his client had been entrapped, "Others on the tapes would refer to my client as 'the kid.' " The defendant was acquitted (Marks 1995).

10. (p. 209) "In attacking Mr. Fortier today, the defense played recordings of a series of his telephone conversations that were wiretapped by Federal agents in the weeks immediately after the bombing, when Mr. Fortier himself was considered a possible suspect. In those recordings, turned over to the defense as part of a pretrial process, he boasted that he could mislead Federal agents and make a million dollars through book rights from his connection to Mr. McVeigh." (Brooke

1997b) Fortier was the lead witness against McVeigh, who was charged with bombing the federal building in Oklahoma City.

11. (p. 210) Elimination of supplies from one area leads to increased cultivation elsewhere (Reuter 1985, pp. 90–93). Increased law enforcement in northern California led to marijuana growing shifting to Kentucky (Kleiman 1993, p. 284). The success of the "French Connection" case caused a significant reduction in the flow of heroin into the United States from Turkey but within three years this was replaced by heroin from Mexico and Southeast Asia (Moore 1990, p. 136). When US efforts eliminated Mexican marijuana, the drug was replaced almost instantly by hemp from Colombia that turned out to be significantly more potent than the Central American variety (Reuter 1985, pp. 91–92).

Simple arithmetic makes clear an additional reason for the failure of interdiction: drugs that are valued at $2000 per pound where they are grown end up costing well over $100,000 per pound on American streets (Rydell 1994, p. 11). The profit margin is sufficiently high and the demand by addicts sufficiently inelastic that seizures have little effect on the commerce in drugs.

12. (p. 211) This is to achieve a 1% reduction in current annual consumption (Rydell, p. xiii). Treating all heavy users once each year would reduce US consumption of cocaine by half in fifteen years and by less than half in earlier years (Rydell, p. xix).

13. (p. 211) Over the years, FBI Directors and Attorneys General have been eloquent in their appeals for electronic surveillance.

> "I dare say that the most violent critic of the FBI would urge the use of wire tapping techniques if his child were kidnapped, and held in custody." [Hoover 1950, p. 230]
>
> "[E]very Attorney General over the last twenty-two years has favored and authorized wire tapping by Federal officials in security cases and other heinous crimes such as kidnapping. . . ." Attorney General Herbert Brownell, in [Brownell 1954a, p. 201]
>
> "By way of background, telecommunications systems and networks are often used to further organized crime, racketeering, extortion, kidnapping . . ." Assistant Attorney General Lee Rawls to Speaker of the House Thomas Foley in 1992 [Rawls 1992]
>
> "Wiretapping is used in the most important life and death cases—terrorism, espionage, drug trafficking, organized crime, kidnapping, and a variety of other crimes" FBI Director Louis Freeh, testifying to Congress in hearings on the digital telephony bill [USS 103b, p. 6]
>
> Freeh was speaking of digital telephony and wiretapping when he told the committee, "I sat last week with Polly Klaas' father [Polly Klaas was the victim of a kidnapper], who came from California to talk to me, and he said to me, 'Mr. Freeh, the FBI did everything in that case to find my little girl.' I do not want to be in a position where I am going to tell some father I could

> not do everything I would normally do because I could not get the access that I have today." [USS 103b, p. 13]

In fact, as the Director well knew, wiretapping would not have prevented Klaas's murder.

14. (p. 211) Approximately at the time that the FBI began its hard push on CALEA, the use of electronic surveillance in kidnapping cases saw a sharp increase. During the period 1968–1993, there were a total of 69 court orders for electronic surveillance. In 1994 the number jumped to 11 kidnapping cases using electronic surveillance and in 1995 to 25. Much is heard about how carefully the courts review electronic surveillance applications but it is striking to note that of the 11 court orders in kidnapping cases, there were 2 surveillances that were never installed and two that were installed but yielded no incriminating intercepts. Furthermore, 2 of the kidnapping cases (one of which did not have an intercept installed) were related to other cases investigated through wiretaps.

The 1995 kidnapping cases show the same pattern: 1 intercept was not installed, 10 had no incriminating intercepts and 2 of the cases (1 installed, 1 not) were related to gambling cases already being investigated through wiretaps. Thus of the 25 so-called kidnapping electronic surveillances, at most 13 yielded any information in a kidnapping case. Installed surveillances that yield no incriminating intercepts are rare, and the kidnapping cases before 1994 do not show this pattern.

15. (p. 211) According to the FBI, the precise numbers are 1990:624; 1991:481; 1992:495; 1993:401; 1994:418 (Source: Michael Kortan, Unit Chief, FBI National Press Office, private communication to Susan Landau, August 7, 1995).

16. (p. 211) This is an area in which improvements in telecommunications have made investigation easier and kidnappers' lives riskier. The familiar process of trying to keep the caller talking long enough that the line can be traced is often made unnecessary by caller-ID mechanisms that reveal the calling number immediately. When this is coupled with *911 databases* that give police information about the locations of phone numbers, it means that even a kidnapper who calls from a phone booth must talk fast and leave quickly.

17. (p. 211) Administrative Office of the United States Courts, *Wiretap Report*, Government Printing Office, Washington, DC, for the years 1988–2005.

18. (p. 212) Source: private conversation between Landau and Iglehart, January 16, 1997.

19. (p. 212) The Los Angeles police had been engaging in 'hand-offs,' in which the first set of investigators, when they discover illegal activity from a wiretap, pass the information on to a new set of investigators without revealing the source. The second set of officers then establish probable cause in order to obtain a new wiretap warrant. In this procedure, the accused would *not* be informed that their case originally developed from wiretapped information (NYT 1998a). When this

practice was uncovered in 1998, the Los Angeles Police Department (LAPD) said it would adopt an interim policy of notifying defendants if their cases involved wiretaps (NYT 1998a).

20. (p. 212) The Administrative Office of the US Courts releases annual reports on wiretaps. In late spring of each year, data become available on the electronic surveillances of the previous year (except for those still in use) as well as new information on previous surveillances. It typically takes about four years for cases involving wiretaps to wend their way through the court system; thus we have picked 1988 as a year to study, since that leaves a sufficiently long window.

21. (p. 213) The Wiretap Reports show arrests through 1996 in cases involving wiretapping investigations in 1988. After 1996, there were no additional arrests or new court cases.

22. (p. 213) These statistics are based on the raw data provided in the *1994 Wiretap Report*. Although the "Reports by Judges on Court Authorized Intercepts" are supposed to be exact data, some of the reports appear instead to be estimates (presumably supplied by the prosecutors). For example, on pages A36–A37, cases AO 471*, 472*, 473*, and 474*, list 2000, 1500, 300, and 1000 intercepts and 100, 300, 200, and 200 incriminating intercepts respectively. This seems unlikely. On pages A38–A39, AO 475* lists 2000 intercepts, of which 500 are recorded as being incriminating. Similarly, on pages A90–A91, cases AO 13, 14 and 15 list 6200, 1200, and 200 intercepts, and 180, 80, and 60 incriminating intercepts respectively. There are a number of other such anomalous figures in the *1994 Wiretap Report*.

23. (p. 213) For this statistic, we are including court authorizations that are solely for wiretaps and not for combination wiretap and electronic bug surveillance.

24. (p. 215) (Public Law 106-197), Continued Reporting of Intercepted Wire, Oral, and Electronic Communications Act.

25. (p. 215) One possibility is that encoding mechanisms that would not be though of as cryptography by security professionals have been reported as such. This would seem more plausible, however, if law enforcement were reporting that it had had difficulty with encryption rather than that it had not. If a data-compression encoding, for example, had been mistaken for encryption but subsequently unscrambled, the initial misunderstanding should not have found its way into the subsequent report. Perhaps, the encryption in question has been done by hand rather than by machine—emails or phone calls containing code words for activities. Another possibility is that the commercially available encryption tools are poorly implemented and permit the plaintext to be recovered without confronting the encryption directly. When encryption is used to protect files on disks, great care is needed to avoid leaving accidental plaintext copies unexpunged. Using encrypted email, it is possible to encrypt the message to some addressees and fail to encrypt those to others.

The most interesting possibility is that there is an unadvertised law-enforcement program for dealing with encrypted communications. This might take several forms. Secure telephony can always be bypassed by installing bugs in or near the telephone or on the line near the telephone. Both original research and scrutiny of government programs (Kuhn) have shown that interception of compromising emanations, particularly by active techniques, is a richer field than is generally imagined. Similarly, the use of encrypted email can frequently be bypassed by installation of spyware, keyboard loggers, and local packet sniffers.

Carrying this speculation a step further, it is possible that the available tools have been compromised either in individual instances or *en masse*. Even where security products are open-source, adequate security evaluations are difficult to conduct initially and difficult to maintain as the products evolve. Typical users "upgrade" their software when upgrades or packages are offered, without even thinking of the possibility that they may have been targeted for a Trojan horse.

26. (p. 216) Table 6 in the appropriate *Wiretap Report*. In using the summary tables of the *Wiretap Report*s one loses specificity; the numbers cited are the sum of all surveillances (phone, electronic, and combination) that are not purely microphone.

27. (p. 216) Annual Department of Justice letter to the Chair of the House Judiciary Committee, as reported in (Burnham 1996, p. 159).

28. (p. 216) Most calls, regardless of distance, now "arrive" with indication of the calling number. This information is often blocked from going to the subscriber but it is available to the local telephone switch and thus to law enforcement.

29. (p. 216) At the time of Foster's death, Clinton's friends and advisors had been scattered across the continent. Had they instead been down the hallway, these conversations—five-minute discussions—might have disappeared into dust. But with hard records of when phone conversations took place, political Washington drew all sorts of conclusions.

30. (p. 216) An exception occurs if there is an emergency; in that case, a court order authorizing the tap must be approved within 48 hours, or all oral and wire communications intercepted in violation of Title III cannot be used in evidence—or even divulged (Omnibus Crime Control and Safe Streets Act, §2515).

31. (p. 217) Source: private conversation between Diffie and Charney, 1975.

32. (p. 217) One possibility is to relax the minimization requirement but increase the reporting requirement by requiring recording of all conversation on a tapped line and making the entire body of material available to the wiretap victims at the close of the investigation, whether or not that investigation leads to a prosecution.

33. (p. 218) Source: private conversation between Diffie and Charney, 1975.

34. (p. 219) Communications Assistance for Law Enforcement Act, Public Law 103-414.

35. (p. 220) One such example is Freeh's reference to the Tina Isa murder (Bryant 1993), which had been recorded by an FBI bug—not wiretap.

36. (p. 220) "Coincidentally, Director Freeh, with your testimony today the *Philadelphia Inquirer* has a major story on 'FBI Nets Stanfa in Mob Sweep,' and the subheadline is 'FBI's Rich Harvest is a Tale of the Tape,' which could not come at a more opportune time to underscore the kind of need of which you are testifying," Specter said (USSH 103 *Digital Telephony*, p. 46).

But the Stanfa case is described in detail in several newspaper articles and the surveillance used is microphone bugs, including one planted in Stanfa's lawyer's office in Camden, New Jersey (Anastasia 1994; Hinds 1994). The case corresponds to AO number 230 in the *1993 Wiretap Report*; the surveillance is explicitly listed as a microphone bug.

37. (p. 220) CALEA applied only to telecommunications carriers and did not affect companies supplying information services, including electronic mail, and Internet services.

38. (p. 220) This includes not only wiretaps but also dialing and signaling information, including "redirection numbers" (call forwarding, call transfers) and call attempts (including unanswered calls).

39. (p. 221) The FBI did not release information indicating which geographic areas corresponded to which categories.

40. (p. 222) Of course, in 1968, you could not typically trace a call in less than several minutes. Furthermore, tracing a call only tells you the calling phone number. The location of the phone is now available to law enforcement from the databases constructed to support the 911 service but these did not exist in 1968.

41. (p. 222) "The proposed legislation does not seek to expand the current laws." (Freeh 1994b, p. 29)

42. (p. 222) The growth factor varies depending on whether the number is "actual" or "maximal" and whether the interception is for wired or wireless communications. For "actual" wired communications the growth factor is 1.259, for "actual" wireless is 1.707, for "maximal" wired communications is 1.303, and for "maximal" wired communications is 1.621 (FBI 1997b).

43. (p. 222) "Actual" means the number of simultaneous communications intercepts, pen registers, and trap-and-trace devices, that the Attorney General anticipates will be simultaneously conducted in 1998, "maximal" means the maximum number (FBI 1997b).

44. (p. 223) The funding was approved in the "Omnibus Consolidated Appropriations Act," and it provided for funding through a combination of money supplied by various intelligence agencies, as well as $60 million in direct funding. An additional $12 million was provided through unspent Department of Justice funds.

45. (p. 223) *Antiterrorism and Effective Death Penalty Act*, Public Law 104-132. This added subsection (f) to Title 18, §2703.

46. (p. 223) The 1996 Antiterrorist and Effective Death Penalty Act (PL 104-32) empowered the Attorney General to determine whether a group constituted a foreign terrorist group and made this designation immune to subsequent judicial review.

47. (p. 224) Some of the evidence was merely circumstantial, as when demonstrators, who used only a telephone to communicate the particulars, appeared at a march or rally and discovered a police presence, or when members of the government knew about tactics that union officials had decided on a short time earlier (Fitzgerald and Leopold 1987, pp. 27–28). But the ubiquity of such wiretapping was confirmed by the General Treasurer of the Post Office Engineering Union—until 1980 the British Post Office ran the telephone system—who in 1980 said there was much evidence to confirm that the Security Services monitored the calls of union officials during work actions (ibid., p. 29). The activities that have come to light occurred before 1985, when Britain codified the procedure for obtaining a wiretap. However, the British green movement, whose most disruptive tactics consist of blocking road-building projects, has been investigated by the Anti-Terrorist Squad. Like labor activists before them, environmental protesters have found police waiting for them at demonstrations whose venues had been relayed only by telephone (Monbiot 1996).

48. (p. 224) In preparing for the discrimination case, the Chief Constable had wiretaps put on the Assistant Chief Constable's private and work phone lines (the private line being at work but a private line). The case went to the European Court of Human Rights, which ruled, "The Court, bearing in mind that the interception of calls made by Ms. Halford on her office telephones at Merseyside police headquarters, not subject to any regulation by domestic law, appears to have been carried out by the police with the primary purpose of gathering material to be used against her in sex-discrimination proceedings" *Halford v. The United Kingdom*—20605/92 [1997] ECHR 32 (25 June 1997) and awarded the ten thousand pounds in damages plus twenty-five thousand pounds in costs. The more important aspect of this decision was that it brought attention to the lack of codes of practice for police wiretapping (Donohue, p. 1167). The result, however, was most disturbing. Instead of establishing safeguards as required by the European Convention on Human Rights, the government used the opportunity to expand police wiretapping powers (Donohue, p. 1167–1168).

49. (p. 224) It was only in 1985, in response to a European Court ruling that objected to the lack of a clear warrant procedure for wiretaps, that Britain adopted wiretap legislation. Before that wiretaps proceeded through a combination of warrants, executive orders, and even informal requests.

Malone challenged the legality of the wiretap, arguing that (i) telephone users had privacy rights, (ii) the wiretapping violated the European Convention on

Human Rights, and (iii) in the absence of a specific wiretap law, the interception was illegal (Fitzgerald and Leopold 1987, pp. 134–135). The British High Court rejected Malone's arguments but the European Convention on Human Rights, after determining the case was admissible, referred it to the European Court on Human Rights, whose rulings can require governments to correct deficiencies in the law. The European Court ruled that under British wiretap law "it cannot be said with any reasonable certainty what elements of the powers to intercept are incorporated in legal rules and what elements remain within the discretion of the executive ... the minimum degree of legal protection to which citizens are entitled under the rule of law in a democratic society is lacking. ..." (Bailey et al. 1991, p. 803)

Current British wiretap law is significantly less specific than US law governing wiretaps and permits the interception of lines not specified in the warrant if it is believed these are *likely* to make contact with lines that are specified in a warrant (Fitzgerald and Leopold 1987, p. 146). In a surprisingly broad view of circumstances that can justify wiretap surveillance, the 1985 British law allows interception in cases that the Foreign Secretary deems to be necessary "to safeguard the economic wellbeing of the country." (Command 9438, paragraph 10, as cited in (ibid., p. 148))

An Independent Commissioner provides an annual report on wiretapping activity to Parliament, but this report is relatively superficial, not even providing the number of intelligence wiretaps (Donohue, p. 1159).

50. (p. 224) See "Interception of Communications," Report to COREPER, ENFOCO 40, 10090/93, Confidential, Brussels, 16.11.93, as reported in "European Union and FBI Launch Global Surveillance System," (Statewatch, London).

51. (p. 225) "Memorandum of Understanding concerning the lawful interception of telecommunications," ENFOPOL 112, 10037/95, Limite, Brussels, in "EU and FBI" (see preceding note).

52. (p. 225) Correspondence with Ministers, 9th Session 1995–1996, HL 74, pp. 26–29, in "EU and FBI."

53. (p. 225) Draft letter to non-EU participants in the informal international Law Enforcement Telecommunications Seminar regarding the Council Resolution, ENFOPOL 180, 11282/96, Limite 6.11.96, in "EU and FBI."

54. (p. 225) "Legally permitted surveillance of telecommunications systems provided from a point outside the national territory," Report from the UK delegation to the Working Group on Police Cooperation, ENFOPOL 1, 4118/95, Restricted, 9.1.95, Report from the Presidency to the Working Group on Police Cooperation, ENFOPOL 1, 4118/2/95 REV 2, Limite, 2.6.95, in "EU and FBI."

55. (p. 227) For example, Louis Freeh testified to Congress on May 19, 1994 that "The proposed [Digital Telephony] legislation relates solely to advanced technology, not legal authority or privacy. It has nothing to do with the separate, but important, 'Clipper Chip' technology." (Freeh 1994c)

56. (p. 227) This took place at a conference on Global Cryptography in Washington, D.C.

57. (p. 227) The memo is dated January 17, 1991 but from context it is clear that the correct date is January 17, 1992.

Chapter 9: Cryptography in the 1990s

1. (p. 231) This committee has since been reconstituted as the Information System Security and Privacy Advisory Board with expanded scope.

2. (p. 231) Raymond Kammer, acting director of the National Institute of Standards and Technology, and Clinton Brooks, assistant to the director of the National Security Agency, briefed the FBI on the dangers encryption posed to wiretapping technology; see Chapter 8.

3. (p. 231) For example, the NSA Director wrote to Dr. Willis Ware, chair of NIST's Computer System Security and Privacy Advisory Board that, "The National Security Agency has serious reservations about a public debate on cryptography." (McConnell 1992)

4. (p. 232) According to one of the NSA "flag badges," NSA's Deputy Director for Operations went looking for the Deputy Director of Information Security with a TSD (telephone security device) in hand. At an encounter in the hall, he rammed the TSD firmly into his opposite number's stomach as though he were passing a football and said: "What are you trying to do to me?" (Subsequent to first publication, I have been told on equally good authority that this could not have happened because the DDO just wasn't the sort of person to do such a thing.—WD)

5. (p. 232) The original producer was RCA's COMSEC division in Camden, New Jersey, which was bought by GTE and later absorbed into Lockheed Martin.

6. (p. 232) Use of the STU-III in secure mode is controlled by an "ignition key," a 64-kilobit storage device packaged in the form of a small plastic key. One key may authorize its holder to use as many as 8 different phones, and as many as 32 distinct keys may be used in any one phone.

7. (p. 233) In addition to new developments, some STU-IIs remain in use, and Clipper phones have official status if not much market share. STU-IIs are also used in parts of NATO and some of our allies have secure-phone systems of their own: Brent in the UK, and Speakeasy in Australia, for example.

8. (p. 233) In fact it had a second signal processor dedicated as a modem, but this was a big improvement on earlier secure phones, some of which had seven.

9. (p. 235) Originally, this was more candidly entitled the Law Enforcement Exploitation Field (LEEF), a phrase consistent with standard SIGINT terminology. The less accurate term "access" was adopted for marketing reasons.

10. (p. 235) The natural question arises: Why not escrow Type I keys? Such a proposal is in line with the standard command and control objective, so carefully sought in the nuclear field, of denying the use of captured weapons to an opponent and may ultimately be undertaken. At present, however, there are hundreds of thousands of Type I devices in the field and any prompt conversion is out of the question. All known forms of key-escrow, moreover, harbor potential vulnerabilities. Introducing key escrow technology first in Type II equipment provides a less sensitive environment in which to refine the techniques.

11. (p. 236) Although the standard was announced on April 16, 1993, it was first published in the *Federal Register* on July 30. The public comment period ran through September 28 (USDoC 1993).

12. (p. 236) The Department of Energy, the US Agency for International Development, and the Nuclear Regulatory Commission all submitted letters opposing the adoption of the Clipper standard.

13. (p. 237) "Authorized implementations may be procured by authorized organizations for integration into security equipment." (USDoC 1994b, p. 6004)

14. (p. 237) There is also be a vulnerability associated with each individual chip. No tamper-resistant technology seems likely to be immortal. At some point, recovery of the device unique key from an individual chip may become economical, rendering each device a threat to all the past traffic it was used to transmit.

15. (p. 237) NSA, however, doesn't seem worried. In early 1996, Fortezza cards were authorized for SECRET traffic and NSA officials used the TSD 3600 to stay in touch with their offices while traveling. (I have subsequently been told that authorization was only for compartmentation in an already-adequately-protected system, so perhaps NSA's faith was all that great.—WD)

16. (p. 238) Federal procurement practices generally combine a standard with a process for approving exceptional requirements. The object is to lower costs through volume purchases resulting from conformance to the standards. Getting approval for exceptions can therefore be very tedious.

17. (p. 239) Source: private conversation between Diffie and AT&T personnel.

18. (p. 239) This lack of confidentiality led to the embarrassing problem Speaker of the House of Representatives Newton Gingrich faced in January 1997 (Lacey 1997).

19. (p. 239) By the early fall of 1992, industry groups working on secure computing had been promised a "Type IIE" cryptosystem—a system with an 80-bit key that would be certified for protecting sensitive government information, but would also be exportable—and had been told the names Skipjack and Capstone. This appears to have been the main program and was probably planned to handle voice traffic among other things. The more limited Clipper program seems to have been pushed forward to accommodate the needs of AT&T's new secure telephone.

20. (p. 239) The name Tessera was taken from a form of "ID" used by the Roman empire to identify subject peoples. Many people considered this a fitting name, but it seems to have been dropped due to an unforeseen trademark infringement.

21. (p. 240) These two principles, taken together, were widely regarded as a show stopper, because a receiving email agent does not transmit and thus has no way of making up for the sender's failure to include an escrow field.

22. (p. 240) The Department of Justice representative even said they would probably have to have SECRET facility clearances.

23. (p. 241) This idea was first put forth by Silvio Micali at Eurocrypt '94 in Italy. His point was that if you want to get something from the user (the escrowing of his key) you have to demand it at a point where the user is getting something he cannot do for himself. Since privacy can be manufactured on an end-to-end basis by a pair of users and authenticity cannot, the service that provides users with letters of introduction, the key management infrastructure, is an appropriate place to attach the string.

24. (p. 242) There was an announcement in early 1997, however, that the earlier form of key escrow was being removed and replaced with the commercially oriented "key recovery" techniques (O'Hara 1997).

25. (p. 242) These were Top Secret Special Intelligence or TS/SI clearances. The three who chose not to go through the process were Colin Crook, Leslie Gelb, and Raymond Ozzie.

26. (p. 243) The other panelists were Lee Bollinger, Colin Crook, Samuel Fuller, Leslie Gelb, Ronald Graham, Martin Hellman, Julius Katz, Peter Neumann, Raymond Ozzie, Edward Schmults, Elliot Stone, and Willis Ware.

27. (p. 243) Even opponents of publicly available strong unescrowed encryption agreed that this was the case. The FBI testified to the NRC panel "the use of export controls may well have slowed the speed, proliferation, and volume of encryption products sold in the US" (Dam and Lin 1996, p. 138).

28. (p. 244) The degree of success that the US lobbying has achieved in Britain should not be surprising. Cryptologic cooperation between the two countries which began during World War II and was later codified into the UK-USA Treaty (Richelson 1985).

29. (p. 245) The hostility to privacy in British law has spread beyond cryptography. A recent law vastly expands police powers of search and virtually removes judicial oversight.

30. (p. 245) Members of the OECD are: Austria, Australia, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, South Korea, Luxembourg, Mexico, New Zealand, the Netherlands, Norway, Poland, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

31. (p. 245) OECD recommendations form the basis for privacy laws in more than a dozen European and Pacific Rim nations (Rotenberg 1996, p. 5).

32. (p. 245) Source: private conversation between Landau and Deborah Hurley, April 3, 1997.

33. (p. 246) In an ironic twist, in early 1997 the German company Brokat Informationssysteme proposed that it ship its strong cryptography systems to the United States, where they would be embedded in products to be exported. Arguing that the shipment from the United States would simply constitute returning the strong encryption to its original markets, Brokat sought to circumvent the restrictive export controls imposed by the US government (Andrews 1997).

Chapter 10: And Then It All Changed

1. (p. 249) The overtly foreign submissions were: LOKI97 from Australia, Rijndael from Belgium, CAST-256 and DEAL from Canada, FROG from Costa Rica, DFC from France, Magenta from Germany, E2 from Japan, CRYPTON from Korea and Serpent from the U.K., Israel, and Norway. The domestic submissions were: MARS, RC6, SAFER+, Twofish, and the Hasty Pudding Cipher, the only purely US entry.

2. (p. 250) IBM, which designed the Data Encryption Standard, built the algorithm to be secure against differential cryptanalysis as later described by Don Coppersmith (Coppersmith). DES is not optimal against linear cryptanalysis, developed by Mitsuru Matsui (Matsui) in 1994, which appears not to have been anticipated by IBM. The earlier history of linear cryptanalysis is not clear. It is essentially the technique the British used to attack the high-grade (above the level of Enigma) German systems during World War II and is implicit in NSA work in the 1960s (Rothaus) but the NSA evaluators do not seem to have imposed it on the design of the DES S-boxes.

3. (p. 252) Neal Koblitz has been a radical since college and was one of the protesters who sat in at the Communications Research Division (now called the Center for Communications Research) of the Institute for Defense Analyses, a research organization that works entirely for NSA, when he was a graduate student in mathematics at Princeton. A few years after his cryptographic discovery, Victor Miller left IBM to take a position at this same laboratory.

4. (p. 252) Elliptic-curve cryptography does not provide a direct replacement for the RSA cryptosystem; instead its key management and signature functions are performed by an Elgamal-type signature and elliptic-curve Diffie-Hellman.

5. (p. 253) In practice, what is required is that it be impossible to alter a message so that its message digest remains unchanged—the *second preimage* problem. For safety, message digests are only considered secure if there is no known way of finding any two messages with the same digest.

6. (p. 253) A feat repeated by the public community shortly thereafter (Chabaud 1998).

7. (p. 253) The work required to find two messages that hash to the same digest can never be greater than that of the workfactor of a cryptosystem whose key is half the size of the hash algorithm's output. SHA-1 with its 160-bit output was designed to have a workfactor of 2^{80}. The later algorithms were designated SHA-256, SHA-384, and SHA-512 and were designed to have workfactors of 2^{128}, 2^{192}, and 2^{256} respectively.

8. (p. 254) Although less than one might have hoped for or expected in half a century.

9. (p. 255) *Daniel Bernstein v US Department of State*, 922 F. Supp. 1426, 1428–30 (N.D. Cal. 1996)

10. (p. 255) *Bernstein v US Department of State* 176 F. 3d 1132, 1141, rehearing en banc granted, opinion withdrawn, 192 F. 3d 1308 (9th Cir. 1999)

11. (p. 255) Since commercial communications play a large and growing role in government communications (both military and nonmilitary), they are a legitimate target of traditional national intelligence collection. The US-government position is that it does not provide covert intelligence information to US companies, but will make use of such information in helping them to counter what it considers foreign corrupt practices.

12. (p. 256) The Administration's anti-cryptography policy was inimical to Silicon Valley, whose support was seen as crucial for the Vice President's bid for President.

13. (p. 257) Information in transit is not considered valuable; if it gets lost, you resend it. If the recipient can't decrypt it, you may have to renegotiate keys and resend. Communications keys are destroyed on a schedule that takes account of what might have been encrypted in them. By contrast, if you depend on cryptography to protect stored data, the keys are just as valuable as the data they were used to encrypt and are valuable for as long as you want the data. Robust availability of the key is therefore the single most important point in management of storage keys.

14. (p. 258) The *Electronic Key Management System* or *EKMS* is a key-management system built by NSA to serve the needs of national security communications. Keys are manufactured at the *central facility* in Finksburg Maryland. When cryptographic equipment is first installed, keys are distributed to it in physical form. After that devices are generally keyed electronically, a process called OTAR or Over the Air Rekeying.

The keying process for the STU-III telephone (currently being phased out in favor of an ISDN phone called the STE) is typical. Shortly after a user receives a new phone, the user receives a small memory device containing a *seed key* usable only for communicating with the central facility. The user makes a secure call to

a special number and the seed key is replaced by operating key, which can be used to call other STU-IIIs. Subsequent changes of key are done in the same way.

The EKMS makes extensive use of public-key technology. In the terms of the commercial world, it plays the role of a certifying authority. Because the military world is smaller and more centralized than the commercial, the EKMS operates as a single level keying hierarchy in which the central facility is the only certifying authority.

In testimony before the Senate in May of 1994 (McConnell 1994) John Michael McConnell, Director of NSA, stated that the Key Management Facility had cost fourteen million dollars to build and would cost sixteen million dollars a year to run.

15. (p. 258) The fact that the memorandum from the Office of Management and Budget was a "recommendation" rather than a "requirement" might look like a weak action but, in fact, given that noncompliance would result in action from an agency's Inspector General, the force of the OMB recommendation is actually as strong as a requirement.

16. (p. 259) How widespread a cryptosystem is depends some on how you count and four obvious measures come to mind. The first is the number of devices. If this is the measure, either SSL in browsers or cryptography in smart cards seem likely to win. Another is total investment, perhaps a smaller number of expensive devices (high-speed trunk-line encryptors, for example) cost more than many cheap ones. A third possibility is the number of bits encrypted. Once again it is possible that a smaller number of highspeed devices will exceed the total traffic volume of a larger number of slow ones. Finally, one might ask if the devices are really used. SSL is in every browser but comparatively few servers operate securely, so the use of SSL is not as great as the browser base suggests.

17. (p. 259) Drugs are an example of a product with a high cost of development and a low marginal cost of production but a high marginal cost of reproduction.

18. (p. 260) http://www.dvdcca.org

19. (p. 262) Ferguson's fears may have been reasonably founded, considering what happened to Dmitry Sklyarov, who was arrested while visiting the US to talk about flaws in the security of e-books at Defcon (McCullagh 2001a).

20. (p. 262) Under California law, because the research was done by state employees in the normal conduct of their duties, the legal team would defend the researchers in any civil action.

21. (p. 262) DMCA §1201 (g) (2) (C).

22. (p. 262) Private conversation between Landau and David Wagner, August 7, 2006.

23. (p. 263) Attestation appears to be due to John Manferdelli of Microsoft but does not seem to have been published outside of the TCG documentation. (Source: conversation between Diffie and Manferdelli, November 9, 2004)

24. (p. 264) Tighter control of enterprise networks will have the socially significant effect of reducing the power of the employees who use them. In the era of timesharing, all control was central. PCs empowered users of all kinds with the ability to configure their machines as they saw fit and to run what programs they wished. Gradually, the PCs owned by corporations have been brought more tightly under the control of corporate IT departments or replaced by centralized servers providing "second generation timesharing."

25. (p. 264) The authors are grateful to Scott Rotondo of Sun Microsystems for pointing out this particular example.

26. (p. 266) English, at 312 million people, is the native language of 30% of Internet users, while Chinese, at 132 million, is the native language of just under 13% (http://internetworldstats.com/stats7.htm, last viewed 18 July 2006). The percentages will undoubtedly shift in the direction of Chinese as more members of that populous nation go online.

27. (p. 266) XML makes up for one of HTML's most glaring defects: HTML has no definitions; a sequence repeated over and over in an HTML document must be repeated over and over; it cannot, as in most computer languages, be abbreviated into a macro or routine.

28. (p. 267) In particular, see (Saltzer), "The function in question can completely and correctly be implemented only with the knowledge and help of the application standing at the endpoints of the communications system. Therefore, providing that questioned function as a feature of the communication system itself is not possible."

29. (p. 268) When I arrived at Sun in 1991, I was asked to choose a name for my workstation, a task I took unreasonably seriously. I departed the day after I was hired for the Crypto conference in Santa Barbara and during the trip stayed with friends in Los Angeles. My hosts obligingly connected to Sun and printed out a list of all the computers on its network, so that I would know what names had been taken. This would not be so easily done today.—WD

30. (p. 269) Information about Carnivore became public as a result of an FBI effort to install Carnivore at the ISP Earthlink. Originally Earthlink was served with an order for a pen register to be installed. Despite the ISP's efforts to carry out the order—Earthlink provided the FBI with headers of incoming mail and some headers of outgoing mail—the FBI was not satisfied and sought to install Carnivore at Earthlink. Earthlink opposed this and went to court, but lost (*In the Matter of an Application of the United States of America for an Order Authorizing the Installation of a Pen Register and Trap and Trace Device*, United States District Court, Central District, Western Division - California, Criminal No. 99-2713M). Part of the difficulty was that the installation of Carnivore crashed Earthlink's remote servers (Wingfield). Earthlink's lawyer, Robert Corn-Revere, testified to the House Judiciary Committee on the issue (Corn-Revere). As a result of his testimony, Carnivore became public.

31. (p. 269) Carnivore was part of the "Dragon Ware" suite of FBI computer programs for Internet surveillance, which included "Packeteer" and "CoolMiner." Packeteer took the data from the raw packets and reconstructed the original format of the communications, while CoolMiner organized the information in a user-friendly manner, so that an investigator could see a target's steps browsing the web, sending email, chatting via ICQ, Yahoo Messenger, AIM, IRC, etc.

32. (p. 270) Bellovin et al. noted that in pen register mode, Carnivore captured lengths of various communications. This allows a certain type of traffic analysis, namely, "[I]n the case of a user visiting a web site, knowing the length of the objects returned can often be used to identify which web page he was visiting (at least for static HTML content), and this is clearly not authorized in pen mode" (Bellovin 2000, itemized comment on 4.2.8).

33. (p. 270) Earthlink objected; see note 30 above.

34. (p. 271) The setting should have been entered in the Carnivore filter set by FBI agents who were detailed to work on Carnivore and who were the only FBI personnel given logical access to the Carnivore appliance. The agents in charge of an investigation should not have had access to the appliance itself but should have been required to make written requests for such changes to the "Carnivore agents."

35. (p. 271) A group of computer-security researchers reviewed the IIT review, and found it sorely lacking (Bellovin 2000). They objected to the lack of systematic review of system issues (flaws that arise when two complex systems interact), lack of systematic search for bugs (especially for string buffer overflows, a well-known problem), and an "inadequate discussion of audit and logging."

36. (p. 271) The Electronic Privacy Information Center discovered in 2002 that this design flaw caused serious consequences. Apparently while the FBI's UBL unit —UBL is the US government's abbreviation for Usama bin Laden—was conducting FISA surveillance, "The software was turned on and did not work properly. The FBI software not only picked up the E-mails under the electronic surveillance of the FBI's target [redacted] but also picked up E-mails on non-covered targets. The FBI technical person was apparently so upset that he *destroyed* all the E-mail take, including the take on [redacted] under the impression that no one from the FBI [redacted] was present to supervise the FBI technical person at the time"(FBI 2000).

37. (p. 273) In principle anything that runs over TCP, or Transmission Control Protocol, which is the Internet's transport-layer reliable transport protocol, can run on Tor.

38. (p. 273) Source: private conversation between Landau and Roger Dingledine, August 11, 2006.

39. (p. 273) Beginning in 2004, work on Tor has also been supported by other government agencies and nonprofits including the Electronic Frontier Foundation.

40. (p. 273) See the discussion regarding data retention in chapter 11.

41. (p. 273) Source: private conversation between Landau and Roger Dingledine, August 11, 2006.

42. (p. 274) http://www.projectliberty.org

43. (p. 275) Disclosure: both authors have worked on the Liberty protocols.

Chapter 11: Après le Déluge

1. (p. 279) Available at http://www.opsi.gov.uk/acts/acts2000/20000023.htm (last viewed October 14, 2006).

2. (p. 280) 50 USC 1801 et seq.

3. (p. 280) Because the CIA had determined that Khaled al-Mihdhar and Nawaf al-Hazmi participated in a meeting in Malaysia with planners of the USS Cole plot, the agency linked the two men to al-Qaeda in 2000 but did not inform the FBI of this. The men were not placed on a "watch list" and were allowed to enter the United States, which is where they were during the summer of 2001. Both men were among the hijackers of American Airlines flight 77 on September 11.

4. (p. 280) USA PATRIOT Act, Pub. L. 107-56. This act is often referred to as the Patriot Act.

5. (p. 280) §218 of PATRIOT Act modified 1804(a)(7)(B).

6. (p. 281) Zacarias Moussaoui was a suspicious French national of Moroccan descent who took flying lessons in Minnesota in 2001. After Moussaoui behaved oddly at flight school, his instructor called the FBI, who arrested Moussaoui on a visa violation. FBI Special Agent Colleen Rowley sought a FISA warrant to search Moussaoui's personal belongings (including his computer), but the FBI was unwilling to apply for a FISA warrant. On September 11, a criminal warrant was issued and Moussaoui was discovered to have connections with al-Qaeda. Moussaoui was later convicted in federal court of conspiring to kill Americans and sentenced to life in prison.

7. (p. 281) As discussed in chapter 8, the Administrative Office of the US Courts publishes an annual *Wiretap Report* that details all electronic surveillance orders of the previous year, including the date surveillance was authorized, how long the surveillance was, who the prosecutor was, who the presiding judge was, how many conversations were surveilled, how many incriminating conversations were surveilled, and whether there were arrests or convictions.

8. (p. 283) In this context "law enforcement officials" refers both to FBI agents and criminal prosecutors (USFISC 2002c, p. 2).

9. (p. 285) Letters containing deadly anthrax spores were sent to news agencies and two US Senators, Tom Daschle and Patrick Leahy (both Democrats, from

South Dakota and Vermont, respectively). Twenty-two people, including postal workers, developed anthrax and five died. For a number of weeks Congressional office buildings were closed while being tested and cleaned.

10. (p. 286) Because information about FISA taps is not public, it is impossible to determine how often a FISA wiretap has been used in what turned into a criminal investigation. We do know that the Justice Department uses the PATRIOT Act tools for investigations of non-terrorists, including: "suspected drug traffickers, white-collar criminals, child pornographers, money launderers, spies, and corrupt foreign leaders and to pursue a broad law-enforcement agenda" for the department has said so (DoJ 2006, p. 56).

11. (p. 286) Offenses under Section 1030 include: intentionally access[ing] a computer without authorization or exceeds authorized access, and thereby obtains[ing] information contained in a financial record of a financial institution, or of a card issuer [or] information from any department or agency of the United States or information from any protected computer if the conduct involved an interstate or foreign communication; intentionally, without authorization access[ing] any nonpublic computer of a department or agency of the United States, access[ing] such a computer of that department or agency that is exclusively for the use of the Government of the United States; knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period.

12. (p. 288) P. L. 109-160, which extended the PATRIOT Act provisions until February 3, 2006, and P. L. 109-170, which extended the provisions until March 10, 2006.

13. (p. 288) §108(a) of P.L. 109-177 amending 50 U.S.C. 1804(a)(3) and 50 U.S.C. 1805(c)(1)(A).

14. (p. 288) This may be extended to sixty days under appropriate circumstances.

15. (p. 288) §108(b)(4) P.L. 109-177, adding 50 U.S.C. 1805(c)(3).

16. (p. 289) The Y2K problem was one of errors caused by computer programs that used 2-digit dates and could not distinguish the year 1900 from the year 2000. Massive checking of legacy programs seems to have found the errors because there were few problems. The disaster many people expected on January 1, 2000 never materialized.

17. (p. 289) Title X, Subtitle G, of P.L. 106-398.

18. (p. 290) Public Law 107-347.

19. (p. 290) In a rather odd situation, there were actually three FISMAs: the Treasury and General Government Appropriations Act for Fiscal Year 2003 FISMA amendment, "FISMA A," and "FISMA B."

The Appropriations Act FISMA had an amendment to extend GISRA past its one-year limit, but by the time the appropriations bill passed, the two other FISMAs had already become law. There was no need for the amendment, which was not folded into the Consolidated Appropriations bill.

FISMA A, Title X of the Homeland Security Act of 2002 (P.L. 107-296), extended GISRA, but put defense agencies in charge of its implementation.

FISMA B, Title III of the E-Government Act was quite similar to FISMA A, but included a provision (§11331 (d)) that placed the Office of Management and Budget, the federal agency responsible for coordinating executive branch management procedures, in charge of implementation.

In signing the E-Government Act, the president designated which bill was operative through a "signing statement" clarifying the implementation of the two laws: "Title III of this Act is the Federal Information Security Management Act of 2002. It is very similar to Title X of the Homeland Security Act of 2002, which also bears the name Federal Information Security Management Act of 2002 and which I signed into law on November 25, 2002. I am signing into law the E-Government Act after the enactment of the Homeland Security Act, and there is no indication that the Congress intended the E-Government Act to provide interim provisions that would apply only until the Homeland Security Act took effect. Thus, notwithstanding the delayed effective dates applicable to the Homeland Security Act, the executive branch will construe the E-Government Act as permanently superseding the Homeland Security Act in those instances where both Acts prescribe different amendments to the same provisions of the United States Code." (Bush 2006)

20. (p. 290) Though cryptography standards are the activity that draw the most public attention, the Computer Security Division's responsibilities are much broader that that. Under FISMA, CSD's role includes developing guidelines for secure system implementation, security research on emerging technologies, and evaluation of security testing labs.

21. (p. 291) For example, the CSD provided cryptographic standards to the banking industry (ISPAB, p. 6) and how NIST provided core technologies that enabled "the [pharmaceutical] industry to create new value" (ISPAB, p. 7).

22. (p. 291) Source: private conversation between Landau and William Barker, September 18, 2006.

23. (p. 292) EZPass is a system in which a user prepays an account using a credit card, personal check, or cash, and receives a small electronic tag for their vehicle, which the driver places on the windshield. This enables the car to drive through specially-equipped toll lanes without stopping. The toll is automatically deducted from the owner's account. EZPass is a system in use throughout the northeastern United States. There are similar systems in other parts of the country and the world.

24. (p. 294) During 1994 hearings, FBI Director Freeh made clear his under-

standing that the bill was limited to telephony systems. In particular, he said, "From what I understand ... communications between private computers, PC-PC communications not utilizing a telecommunications common net, would be one vast arena, the Internet system, many of the private communications systems which are evolving. Those we are not going to be on by the design of this legislation." Senator Larry Pressler asked, "Are you seeking to be able to access those communications also in some other legislation?" Freeh responded, "No, we are not. We are satisfied with this bill. We think it delimits the most important area and also makes for the consensus, which I think it pretty much has at this point." (USSH 103 *Digital Telephony*, p. 202).

25. (p. 294) Communications Assistance for Law Enforcement Act, §102 (8)(C).

26. (p. 294) Communications Assistance for Law Enforcement Act, §103 (b)(2).

27. (p. 295) "CALEA applies to facilities-based Internet access providers and interconnected VoIP service providers" (FCC 2005a, p. 24).

28. (p. 295) It was not only the petitioners who viewed it this way. In his dissenting opinion, Senior Circuit Judge Harry T. Edwards wrote:

> "In determining that broadband Internet providers are subject to CALEA as 'telecommunications providers,' and not excluded pursuant to the 'information services' exemption, the FCC apparently forgot to read the words of the statute." *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, Edwards, dissenting).

29. (p. 295) The petitioners did not completely lose the case; the Appeals Court ruled, for example, that a CALEA exemption remained for private networks, such as those maintained by educational institutions.

30. (p. 295) The authors were part of an industry study (Bellovin 2006a) of the impact of applying CALEA to VoIP and what follows draws heavily on that report.

31. (p. 296) This diagram and discussion first appeared in (Bellovin 2006a).

32. (p. 298) We are glossing over the difficulty of Alice's VoIP Provider even knowing who Alice's ISP is, let alone the location or identity of R1. These are non-trivial issues in and of themselves.

33. (p. 300) In fact the signaling message is sent to the home location register, a database containing the identity and service profile of the subscriber.

34. (p. 300) In spirit an *en banc* review is a review by the full court but in practice, it is review by a panel of judges significantly larger than the original panel of three but smaller than the whole court.

35. (p. 302) The *New York Times* had uncovered the story in 2004, but the White House requested that the newspaper not publish on the subject, "arguing that it could jeopardize continuing investigations and alert would-be terrorists that

they might be under scrutiny." (Risen) The *Times* reporters investigated the issue for another year and then published. The Bush administration began investigations to determine who had leaked the story to the press. Meanwhile the two reporters who broke the story, James Risen and Eric Lichtblau, won a Pulitzer Prize for "carefully sourced stories on secret domestic eavesdropping that stirred a national debate on the boundary line between fighting terrorism and protecting civil liberty." (Pulitzer)

36. (p. 304) The falling cost of storage holds promise of changing this.

37. (p. 304) NessiE material can be found at www.cryptonessie.org.

38. (p. 306) Senator Charles Grassley added, "I worry down the road that ... some prosecutors who do not have experience dealing with terrorists and spies may be tempted to order an arrest for a reason other than national security. That prosecutor may, for instance, want a convicted terrorist on his record, even though it is smarter to watch the suspect and learn about his plans and and conspirators. The intelligence agencies on the case may still be looking for other terrorists in the cells, but they get overruled by the prosecutor.... I am worried that prosecution is not always the best decision in terms of national security." (Grassley, p. 28)

39. (p. 306) On August 6, 2001, the President's Daily Brief contained a two-page memo titled "Bin Laden Determined to Strike in US" that described "patterns of suspicious activity in this country consistent with hijackings" (White House 2001, p. 2)

40. (p. 306) Gary Hart was a Democrat from Colorado, Warren Rudman a Republican from New Hampshire.

41. (p. 307) The policy was dropped because of the lack of measurable success in fighting terrorism (Bernstein 2004).

42. (p. 307) South Asian immigrants in Britain are three times as likely to be unemployed as white Britons and indeed, 40 percent of Pakistani women in Britain are unemployed, as are 28 percent of Pakistani men (Bernstein 2006). The situation in the United States is markedly different: incomes of people of Pakistani origin are close to the median in New York and slightly exceed the median in New Jersey (there is, however, a large underclass of South Asians) (ibid., p. A1). The pattern of Arab Americans follows the pattern of most immigrant groups in the US that have been here for a few generations: Arab-Americans have a higher rate of college and post-college education. The median income of Arab Americans is higher than the US median (Fallows, p. 65).

43. (p. 308) Queensborough Public Library in New York City, which serves an immigrant population, took steps to preserve privacy of patrons, including delinking of electronic book/patron info when book is returned, daily destruction of Internet usage sign-up sheets, etc. (NRC 2006). The message from the Queensborough library is clear: you are part of our society, deserving of our protections.

44. (p. 309) A case in point is the 9/11 hijackers. Mohamed Atta described a nuclear facility as "electrical engineering" to his fellow pilots (National Commission, p. 245). Khalid Sheikh Mohammed used the code of send "the skirts" to "Sally" to instruct another al-Qaeda member to send funds to Zacarias Moussaoui (National Commission op. cit. at 246). The targets were discussed as if the participants were students at a university: the Pentagon was "arts," the World Trade Center, "architecture," the Capitol, "law," and the White House, "politics" (National Commission, p. 248).

45. (p. 309) This realization undoubtedly contributed to NSA acquiescence to the change in cryptographic export-control regulations in 2000.

46. (p. 310) Reid attempted to blow up an American Airlines flight from Paris to Miami by lighting his shoe tongue. Reid's shoes contained an explosive. The attempt was thwarted by a flight attendant. The plane was diverted and Reid was arrested upon arrival in Boston (USDoJ 2006, p. 26).

47. (p. 311) TRAC is a research center at Syracuse University devoted to data collection, analysis and distribution, about federal government staffing, spending, and enforcement activities.

48. (p. 311) On July 30, 1916, in the midst of World War I—but before US participation in the war—a munitions storage depot in New York Harbor was destroyed by saboteurs, destroying over two million pounds of explosives. The blast burst windows in Jersey City, Manhattan, and Brooklyn, and was heard over 100 miles away in Philadelphia. (Landau 1937, pp. 77–91). This was the largest terrorism act during this period, but there were numerous other explosions at industrial plants, all laid at German saboteurs. They were estimated to have caused over $150 million in damage to essential war goods (Sayers, p. 11). There was even an attack at the US Capitol switchboard (Landau 1937, pp. 305–307).

49. (p. 311) In 1994, when FBI Director Louis Freeh testified before Congress in support of the "Digital Telephony" bill (later passed as CALEA), he emphasized the importance of wiretaps in solving kidnappings and in preventing terrorist actions (Freeh 1994b).

50. (p. 311) At the time of Freeh's testimony (1994b), Title III was just turning 25 years old. If wiretaps are an important tool of law enforcement, there should be enough clear-cut cases in 25 years to allow a persuasive case to be made. Freeh's account of the value of wiretapping is remarkably vague. He refers to numerous convictions, without mentioning the name of a single defendant, court, presiding judge, case name, or docket number. This makes the information difficult to verify or explore. It is one thing to say that you can't give the details of ongoing investigations or that cases ended in plea bargains or that crimes were prevented without any trials resulting; it is another to fail to identify cases that must be the results of public trials.

Credence is further strained by the inclusion of at least one identifiable case

—the Tina Isa case—in which the surveillance was a microphone planted in the living room in which a teenage girl was murdered (Bryant 1993).

Chapter 12: Conclusion

1. (p. 314) It has long been an asset of private detectives, often retired police, to have friends in the department who will give them non-public information—looking up addresses from license plate numbers, for example. In the twenty-first century, well-connected detectives may be among the beneficiaries of CALEA and its descendents.

2. (p. 315) Although widespread wiretapping is an abomination, government surveillance is not in all respects undesirable: the government's ability to serve its citizenry is, after all, dependent on sufficient understanding of the population's activities to know the population's needs (Bogard).

3. (p. 315) At the first of the American public cryptographic conferences, Crypto '81, which was held at the University of California at Santa Barbara, one of the NSA people said to me: "It's not that we haven't seen this territory before, but you are covering it very quickly."—WD

4. (p. 315) In the AT&T TSD3600, for example, encryption represents approximately 1–2% of the computation. It is 3% of the cycles of the main processor, but this is assisted by a dedicated modem chip. In short, the TSD spends almost all of its effort either preparing the speech to be encrypted or preparing the cipher text to be sent over the phone line. The rest goes to encrypting it.

5. (p. 315) For example, the GSP8191 secure telephone, was designed by one person, Eric Blossom, in a little more than 2 years. Skype, the secure VoIP system was done by a dozen in a similar length of time.

6. (p. 316) Establishing that the person you are communicating with now is the same person you were communicating with at some previous time is socially fundamental; it is the way acquaintances develop. The ability to assume a persona and to sign email provides a mechanism by which people can meet on the Internet and have some confidence that they are communicating with the same person each time, without exchanging any absolute information about their identities.

7. (p. 316) The Atomic Energy Act of 1954 created the notion that ideas in atomic energy were "born secret" and were to remain secret unless the government said they could be disclosed.

8. (p. 317) In 1992, the FBI's Advanced Telephony Unit warned that by 1995 no more than 40% of Title III wiretaps would be intelligible and that in worst case all might be rendered useless (Advanced Telephony Unit 1992). In 1994 Assistant Attorney General Jo Ann Harris admitted that, a year after the introduction of the Clipper proposal, the FBI had yet to encounter a single instance of encrypted voice communications (Harris 1994). Further data in the *Wiretap Report* for the

years 2000–2005 bears out that encrypted voice communications are simply not a problem.

9. (p. 318) FBI directors have always emphasized the use of wiretaps in kidnapping investigations, and Louis Freeh was no exception. In fact wiretaps were used on average in only two to three kidnapping cases a year in the period 1968–1993. Terrorist actions were likewise cited as an important reason for wiretaps,despite the fact that there were no Title III wiretaps in terrorist cases in the period 1988–1994.

In pressing for various wiretapping capabilities, FBI Assistant Director James Kallstrom argued: "... just for the FBI alone, we have used court-authorized electronic surveillance to capture terrorists intent on blowing up buildings and tunnels in New York, to detect and capture pedophiles who intended to brutally murder their intended victim, to arrest and convict various organized crime leaders like John Gotti, and to successfully investigate a spy whose espionage cost many their lives" (Kallstrom 1997). However, the Rahman case ("terrorists intent on blowing up buildings and tunnels in New York") turned not on wiretaps, but on other forms of electronic surveillance, including a body wire (which does not require a warrant); the valuable evidence in the Gotti case came from an electronic bug (Less than eight months after Kallstrom's remarks, FBI Director Louis Freeh testified to a Senate Judiciary committee hearing: "John Gotti never implicated himself on a telephone conversation with one of his confederates." (USS 105d).); and the wiretap in the Ames case ("a spy whose espionage cost many their lives") served in a tangential fashion, enabling the government to pressure Ames to reveal information in order that his wife—whose knowledge of his spying activities was revealed on the wiretaps—receive a reduced sentence. (The value of the wiretap in the Ames investigation should be placed in context: a recent Department of Justice (USDoJ 1997) report severely castigated the FBI for inadequately investigating the FBI and CIA spy losses years earlier and thus allowing Ames to inflict further damage on US intelligence.)

10. (p. 319) This is a point that Congress might do well to consider amending.

11. (p. 320) Mail covers operated from the 1940s til the early 1970s; copies of telegrams were also sent to NSA during that period. See chapter 6.

12. (p. 320) See chapter 6, and discussions on Kennedy, Johnson, and Nixon.

13. (p. 324) A good example is Anatoli Golitsin, a Soviet defector who initiated a decade long search for "moles" in the CIA.

14. (p. 325) A common division of responsibility in this respect has been that field stations do signal processing on received material, but leave all cryptanalytic operations to be done by headquarters.

15. (p. 325) One fascinating possibility is that the cryptanalysis of some popular cryptographic algorithm such as DES or 40-bit RC4 might be achieved and embedded in a tamper-resistant chip. Intercept equipment with explicit "counter-DES capability" or "counter-RC4 capability" might thereby become available.

16. (p. 325) Some of the uses are commercial. Emitter identification is being used to detect cloned cellular phones (AWST 1997b).

17. (p. 326) The technology that makes this available is the same as that of caller ID.

18. (p. 327) Systems such as *Teletrack* keep track of the locations of fleet vehicles and report this information automatically to a dispatcher. They may even have profiling capabilities that allow them to warn the dispatcher when a vehicle is out of its expected area, behind schedule, etc.

19. (p. 328) By wiretap law—Title III, FISA, and subsequent amendments—communications on these networks are subject to wiretap. The issue is making the network architecture subject to CALEA.

20. (p. 329) Effects of this kind are seen in microcosm in the case of Robert Hanssen, a spy within the FBI, who was able to tap into counterintelligence databases in order to detect whether he was being investigated (United States of America v. Robert Philip Hanssen, Affidavit in Support of Criminal Complaint, Arrest Warrant and Search Warrants.) (United States District Court for the Eastern District of Virginia, Alexandria Division).

21. (p. 329) Source: Greek government press briefing, February 2, 2006. English translation provided by George Danezis http://homes.esat.kuleuven.be/~gdanezis/intercept.html (last viewed October 16, 2006).

22. (p. 330) Personal reminiscence of Gustavus J. Simmons, retired Senior Research Fellow at Sandia National Labs, told to Diffie in 1991.

23. (p. 331) The current government efforts are focused on VoIP. However, there is a draft Department of Justice bill that would apply the CALEA requirements to any real-time communications. This would include Instant Messaging, MMORPGs, etc.

24. (p. 332) French law requires the police to consult the courts when initiating any investigation of a citizen (Kelling 1991, p. 965).

25. (p. 333) Textbooks on criminal investigation devote approximately 1% of their pages to the subject.