NOTES

1 Senate Bill 266, Senators Biden and DeConcini.

2 John Perry Barlow, in "Decrypting the Puzzle Palace," *Communications of the ACM*, July 1992, 35:7, p. 25–31.

3 The historic information in this section is from Alan F. Westin, *Privacy and Freedom*, Atheneum, 1968, Alexander Charns, *Cloak and Gavel: FBI Wiretaps, Bugs, Informers, and the Supreme Court*, University of Illinois Press, 1992 (Chapter 8); Edith Lapidus, *Eavesdropping on Trial*, Hayden Book Co., 1974; and Walter Isaacson, *Kissinger: A Biography*, Simon and Schuster, 1992.

4 *Nardone v. U.S.* 302 U.S. 379(1937).

5 The quote is in the foreword of Lapidus, *Eavesdropping on Trial*.

6 For example: U.S. Department of State, "Country Reports for Human Rights Practices for 1996," Jan. 30, 1997. www.state.gov/www/global/human_rights/hrp_reports_mainhp.html.

7 Mark Leccese, "Telecomputing and the U.S. Constitution: Steve Jackson Games Goes to Trial," *Connect*, May/June 1993, pp. 38–43. "Electronic Publishing, Bulletin Board E-Mail, and the Steve Jackson Games Case," *Legal Bytes*, published by George, Donaldson & Ford, Winter 1992–93, 1:1, p. 5. Dorothy Denning, "The United States vs. Craig Neidorf," *Communications of the ACM*, March 1991, 34:3, pp. 23–32. www.sjgames.com/SS. "10th Anniversary of USSS Raid on Steve Jackson Games & Illuminati BBS," *EFFector*, Mar. 1, 2000, 13:2 (www.eff.org).

8 Robin Hanson, "Can Wiretaps Remain Cost Effective?" *Communications of the ACM*, Dec. 1994, 37:12, pp. 13–15.

9 "Just Published," *Privacy Journal*, June 2000, p. 7. "Federal Wiretaps Stay at High Level," *Privacy Journal*, June 1996, p. 6. Robert Fox, "Newstrack," *Communications of the ACM*, July 1994, 37:7, p. 9. "In Congress: FBI Wiretapping Proposal on a Fast Track," *Privacy Journal*, Sept. 1994, p. 3. Hoffman *et al.*, p. 115. Dorothy E. Denning and William E. Baugh, Jr., "Encryption and Evolving Technologies As Tools of Organized Crime and Terrorism," National Strategy Information Center, 1997.

10 John Schwartz, "Industry Fights Wiretap Proposal," *Washington Post*, March 12, 1994, p. C1, C7.

11 "Overkill By the FBI For New Tapping Authority," *Privacy Journal*, Dec. 1993, p. 3.

12 "Independent Technical Review of the Carnivore System," Illinois Institute of Technology Research Institute, Nov. 17, 2000, www.usdoj.gov/jmd/publications/carniv_entry.htm. David Banisar, "A Review of New Surveillance Technologies," *Privacy Journal*, Nov. 2001, pp. 1, 5–7. www.epic.org/privacy/carnivore/foia_documents.html

13 Guy Chazan, "A High-Tech Folk Hero Challenges Russia's Right to Snoop," *Wall Street Journal*, Nov. 27, 2000, p. A28. Christopher Hamilton, "Russians Fight for Net Privacy," *ABCNEWS.com*, June 12, 1999. The treaty is at http://conventions.coe.int/treaty/EN/projets/cybercrime27.htm. Will Rodger, "Trans-Atlantic Treaty Would Authorize Close Monitoring of Internet Usage," *Privacy Journal*, June 2001, 27:8, pp. 1, 4.

14 Ted Bridis, "FBI's E-Mail Suggests Divisions On Legality of Web Surveillance," *Wall Street Journal*, Dec. 7, 2000, p. B9.

15 Gregory Vistica, "Inside the Secret Cyberwar," *Newsweek*, Feb. 21, 2000, p. 48. The 2001 budget estimate is from the Federation of American Scientists (www.fas.org).

16 James Bamford, *The Puzzle Palace: A Report on NSA, America's Most Secret Agency*, Houghton Mifflin, 1982, p. 12. Testimony of Gen. Hayden. Bamford, *Body of Secrets*, pp. 435–440.

17 Neil King Jr., "As Technology Evolves, Spy Agency Struggles To Preserve Its Hearing," *Wall Street Journal*, May 23, 2001, p. A1, A10.

18 European Parliament, "An Appraisal of Technologies of Political Control," Jan. 6, 1998, and European Parliament, "Interception Capabilities 2000," Apr. 1999. These documents (and others about Echelon) are available at www.privacy.org/pi/activities/tapping. Report of the Temporary Committee on the Echelon Interception System, May 2001, www.europarl.eu.int/tempcom/echelon/pdf/prechelon_en.pdf. Echelonwatch FAQ, www.aclu.org/echelonwatch/faq.html, visited Feb. 7, 2001.

19 James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency, from the Cold War Through the Dawn of a New Century*, Doubleday, 2001, pp. 404, 409.

20 Statement for the Record of NSA Director Lt. General Michael V. Hayden, USAF; House Permanent Select Committee on Intelligence, Apr. 12, 2000. www.nsa.gov/releases/DIR_HPSCI_12APR.HTML.

21 Neil King Jr., "Security Agency Defends Eavesdrop Use," *Wall Street Journal*, Apr. 13, 2000, p. A4. Bamford, *Body of Secrets*, pp. 414–418.

22 R. James Woolsey, quoted in Bamford, *Body of Secrets*, p. 425.

23 Patrick Poole, "'Echelon' Spells Trouble for Global Communications," *Privacy Journal*, Sept. 1999, pp. 3–4.

24 The French government admitted eavesdropping on the communications of American business people and providing valuable commercial information to French companies (Mary Eisenhart, "Encryption, Privacy & Data Security," *MicroTimes*, March 8, 1993, pp. 111–122.)

[25] Larry Loen, "Hiding Data in Plain Sight," *EFFector Online*, Jan. 7, 1993, 4.05.

[26] Steven Levy, "The Open Secret," *Wired*, April 1999, pp. 108–115; Simon Singh, *The Code Book: The Evolution of Secrecy From Mary Queen of Scots to Quantum Cryptography*, Doubleday, 1999, pp. 279–292.

[27] Quoted in Steve Lohr, "Privacy on Internet Poses Legal Puzzle," *New York Times*, Apr. 19, 1999, p. C4.

[28] Lance J. Hoffman, Faraz A. Ali, Steven L. Heckler, Ann Huybrechts, "Cryptography Policy," *Communications of the ACM*, Sept. 1994, 37:9, pp. 109–117.

[29] Fyodor Dostoevsky, *The House of the Dead*, 1862; translation by Constance Garnett, 1915.

[30] David Chaum, "Achieving Electronic Privacy," *Scientific American*, Aug. 1992, pp. 96–101. David Chaum, "A New Paradigm for Individuals Living in the Information Age," in Deborah G. Johnson and Helen Nissenbaum, *Computers, Ethics & Social Values*, Prentice Hall, 1995, pp. 366–373. Julian Dibbell, "Building a Better Monkey Wrench," *Village Voice*, Aug. 3, 1993, p. 34.

[31] Quoted in *EFFector Online*, 7:3, Feb. 9, 1994

[32] Eric Dexheimer, "Police Uneasy with This Cure for the Common Code," *San Diego Union–Tribune*, Computer Link section, March 1, 1994, p. 1ff. Steven Levy, "Battle of the Clipper Chip," *New York Times Magazine*, June 12, 1994, pp. 44–70 (p. 49). Dorothy E. Denning and William E. Baugh, Jr., "Encryption and Evolving Technologies As Tools of Organized Crime and Terrorism," National Strategy Information Center's U.S. Working Group on Organized Crime, 1997. Dorothy E. Denning and William E. Baugh, Jr., "Cases Involving Encryption in Crime and Terrorism," www.cosc.georgetown.edu/~denning/crypto/cases.html.

[33] Niels Provos and Peter Honeyman, University of Michigan Center for Information Technology Integration.

[34] Philip Elmer-Dewitt, "Who Should Keep the Keys?" *Time*, March 14, 1994, pp. 90–91. Julian Dibbell, "Code Warriors Battling for the Keys to Privacy in the Info Age," *Village Voice*, Aug. 3, 1993, pp. 33–37. Singh, *The Code Book*, p. 318. Bamford, *The Puzzle Palace*, p. 4.

[35] Bamford, *The Puzzle Palace*, pp. 356–357, 361–362. The Davida quote is on p. 361.

[36] William Sternow, quoted in Dexheimer, "Police Uneasy with This Cure for the Common Code."

[37] James Bidzos, president of RSA Data Security, quoted in John Perry Barlow, "Decrypting the Puzzle Palace," p. 27. Kimberley A. Strassel, "U.S. Limits on Encryption Exports Create Fans Overseas, *Wall Street Journal*, July 7, 1998, p. B5.

[38] Hoffman et al, "Cryptography Policy," pg. 113.

[39] Paul Wallich, "Cracking the U.S. Code," *Scientific American*, Apr. 1997, p. 42. The book containing the code that could not be exported on disk is *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, by Bruce Schneier, published in 1994. "State Dept: 1st Amendment Doesn't Apply to Disks," *EPIC Alert*, Oct. 28, 1994, v. 1.06. Telephone interview with Philip Karn, March 17, 1995.

[40] Loring Wirbel, "State Dept. Tries to Quash APIs for PGP Cryptography," *Electronic Engineering Times*, Apr. 29, 1996, p. 4. Don Clark, "Sun Holding Off On Plans to Market Encryption Systems," *Wall Street Journal*, Mar. 9, 1998, p. B3.

[41] "EFF Sues to Overturn Cryptography Restrictions," *EFFector Online*, Feb. 23, 1995, 8:2.

[42] Judge Marilyn Patel, quoted in Jared Sandberg, "Judge Rules Encryption Software Is Speech in Case on Export Curbs," *Wall Street Journal*, Apr. 18, 1996, p. B7.

[43] Josh McHugh, "Politics for the Really Cool," *Forbes*, Sept. 8, 1997, pp. 172–179.

[44] Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press 1998, pp. 107–108.

[45] Michael J. Martinez, "New Computer Could Foil Encryption Schemes," *ABCNEWS.com*, May 7, 1999.

[46] Julian Dibbell, "Tale From the Crypto Wars," *Village Voice*, Aug. 3, 1993, p. 36.

[47] Whitfield Diffie and Susan Landau, *Privacy on the Line*, pp. 207–217. See also S. Kent et al, "Codes, Keys and Conflicts: Issues in US Crypto Policy, Report of a Special Panel of the ACM US Public Policy Committee," June 1994 (http://info.acm.org/reports/acm_crypto_study.html).

[48] John Podesta, quoted in "Answers to Clipper Questions," *EFFector Online*, 5:14, Aug. 5, 1993.

[49] Assistant Attorney General Jo Ann Harris, before a Senate Judiciary Subcommittee, May 3, 1994.

[50] The report is titled "Encryption: The Threat, Applications and Potential Solutions." It is quoted in "Documents: FBI & NSA Want to Ban Non-Escrowed Encryption," *EPIC Alert*, Aug. 21, 1995, v. 2.09.

[51] "Impact of Emerging Telecommunications Technologies on Law Enforcement," also quoted in *EPIC Alert*, ibid.

[52] David Kahn, *The Codebreakers*, Macmillan, 1967, pp. 515–517. Dibbell, "Tale From the Crypto Wars." Nathan Aaseng, *Navajo Code Talkers*, Walker & Co., 1992.

[53] Kenneth W. Dam and Herbert S. Lin, eds., National Research Council, *Cryptography's Role in Securing the Information Society*, National Academy Press, 1996 (books.nap.edu/html/crisis).

[54] From the Security and Freedom through Encryption Act (SAFE), as amended by the House Intelligence Committee, Sept. 11, 1997.

[55] Martinez, "New Computer Could Foil Encryption Schemes," Will Rodger, "Cell phone encryption code cracked," *USATODAY.com*, Dec. 8, 1999.

[56] James Bidzos, in Eisenhart, "Encryption, Privacy & Data Security." James Chandler, George Washington University National Law Center, mentioned in Hoffman *et al.*, "Cryptography Policy," p. 115.

[57] "Overkill by the FBI for New Tapping Authority," *Privacy Journal*, Dec. 1993, p. 3.
[58] Jerry Berman and Daniel J. Weitzner, *EFFector Online*, 5:5, April 2, 1993.
[59] Simon Singh, *The Code Book*, pp. 45–78, 317–350.
[60] www.cryptorights.org. Zimmermann quotes from Dexheimer, "Police Uneasy with This Cure for the Common Code," p. 12.
[61] Book report on *1984* written for my course, CS 440, Fall 2000; used with permission.
[62] Eisenhart, "Encryption, Privacy & Data Security," p. 118.

BOOKS AND ARTICLES

- James Bamford, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency, from the Cold War Through the Dawn of a New Century*, Doubleday, 2001. Includes a description of Echelon.
- James Bamford, *The Puzzle Palace: A Report on NSA, America's Most Secret Agency*, Houghton Mifflin, 1982.
- John Perry Barlow, "A Plain Text on Crypto Policy," *Communications of the ACM*, Nov. 1993, 36:11, pp. 21–26.
- Duncan Campbell, "Interception Capabilities 2000," www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm. A report on Echelon to the European Parliament.
- Alexander Charns, *Cloak and Gavel: FBI Wiretaps, Bugs, Informers, and the Supreme Court*, University of Illinois Press, 1992.
- David Chaum, "Achieving Electronic Privacy," *Scientific American*, Aug. 1992, pp. 96–101.
- Robert Corn-Revere, "The Fourth Amendment and the Internet," Testimony before the Subcommittee on the Constitution of the House Committee on the Judiciary, Apr. 6, 2000, www.house.gov/judiciary/corn0406.htm.
- Dorothy E. Denning, *Information Warfare and Security*, Addison Wesley, 1999.
- Dorothy E. Denning, "The Case for 'Clipper'," *Technology Review*, July 1995, pp. 48–55.
- Dorothy E. Denning *et al.*, "To Tap or Not To Tap," *Communications of the ACM*, March 1993, 36:3, pp. 25–44. This debate on wiretapping and encryption policy includes an article by Denning and responses from a variety of points of view.
- Dorothy E. Denning and William E. Baugh, Jr., "Encryption and Evolving Technologies As Tools of Organized Crime and Terrorism," National Strategy Information Center's U.S. Working Group on Organized Crime, 1997.
- Dorothy E. Denning and William E. Baugh, Jr., "Cases Involving Encryption in Crime and Terrorism," www.cosc.georgetown.edu/~denning/crypto/cases.html.
- Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press 1998.
- Dorn, James A., ed., *The Future of Money in the Information Age*, Cato Institute, 1997.
- David Flaherty, *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, 1989.
- Robin Hanson, "Can Wiretaps Remain Cost Effective?" *Communications of the ACM*, Dec. 1994, 37:12, pp. 13–15.

- Lance J. Hoffman, ed., *Building In Big Brother: The Cryptographic Policy Debate*, Springer Verlag, 1995.
- S. Kent *et al.* "Codes, Keys and Conflicts: Issues in US Crypto Policy, Report of a Special Panel of the ACM US Public Policy Committee," June 1994, http://info.acm.org/reports/acm_crypto_study.html.
- Edith Lapidus, *Eavesdropping on Trial*, Hayden Book Co., 1974. Contains history of wiretapping and the relevant sections of the Omnibus Crime Control and Safe Streets Act of 1968.
- Steven Levy, *Crypto: How the Code Rebels Beat the Government—Saving Privacy in the Digital Age*, Viking Press, 2001.
- Wayne Madsen and David Banisar, *Cryptography and Liberty 2000: An International Survey of Encryption Policy*, Electronic Privacy Information Center, 2000.
- National Research Council, *Cryptography's Role in Securing the Information Society*, National Academy Press, 1996, books.nap.edu/html/crisis.
- Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, John Wiley & Sons, Inc., 2000.
- Solveig Singleton, *Encryption Policy for the 21st Century: A Future without Government-Prescribed Key Recovery*, Cato Institute Policy Analysis, No. 325, Nov. 19, 1998.
- Simon Singh, *The Code Book: The Evolution of Secrecy From Mary Queen of Scots to Quantum Cryptography*, Doubleday, 1999. A history of codes and cryptography.
- Alan F. Westin, *Privacy and Freedom*, Atheneum, 1968. Contains history of wiretapping and other means of surveillance.
- Philip R. Zimmermann, *The Official PGP User's Guide*, MIT Press, 1995. Includes discussion of legal, ethical, and political issues surrounding PGP.

ORGANIZATIONS AND WEBSITES

- The CryptoRights Foundation: www.cryptorights.org
- Echelonwatch, sponsored by the American Civil Liberties Union, the Electronic Privacy Information Center, and other organizations: www.echelonwatch.org
- The EFF and EPIC sites, listed at the end of Chapter 2 contain a lot of material about the controversies in this chapter. For example, www.epic.org/crypto
- The Federal Bureau of Investigation: www.fbi.gov
- The National Security Agency: www.nsa.gov