18. Encryption and Wiretapping

Congress should

- lift all technical review requirements for encryption software and hardware;
- reject attempts to foist key escrow, or key recovery, on the market;
- reject a strong federal role in standardizing digital signatures;
- repeal the Communications Assistance for Law Enforcement Act, which treats every U.S. citizen like a suspect and phones as tracking devices; and
- prohibit the FBI from deploying Carnivore-type systems.

New communications technologies, from secure encrypted e-mail to digital and mobile phones, will be the engines of the 21st-century economy, changing every aspect of human life just as the printing press did. Also, the new technologies make wiretaps less useful to law enforcement authorities. Congress should not shackle new technology to preserve a few speculative gains for law enforcement. The costs far outweigh the benefits. Law enforcement can and will adapt to the new world.

Encryption Export Controls

Encryption software enciphers data sent over computer networks, so that only people with special information such as a secret key can read the plaintext of the message. The key is a string of numbers. The longer the string, the harder it is to break. Encryption technology is essential for citizens to preserve their privacy and security when using computer networks. Otherwise, medical records, credit card numbers, trade secrets, and personal communications relayed over computer networks are not safe from prying eyes.

In January 2000 the Department of Commerce announced new encryption export regulations. Under the new regulations, U.S. companies may export any encryption product around the world to private-sector end users or commercial firms (except those in seven terrorist nations) after a one-time technical review. Encryption products that the Bureau of Export Administration (BXA) determines fall into the category of "retail encryption commodities and software" can be exported to anyone. In determining which products fit the definition, the BXA will consider the product's function, sales volume, and distribution methods. Publicly available source code may be exported without technical review.

The relaxation of export controls on products intended for e-commerce merchants, financial institutions, and others is a step in the right direction. But problems remain. First, the "publicly available" or "sales volume" tests doom U.S. companies to lag behind foreign cryptographers in offering new encryption products. No pioneer product is yet "publicly available" or has a large sales volume. The revised encryption rules thus still allow foreign cryptographers to take the lead in developing new crypto products.

Second, any encryption products must be submitted for a technical review before release. This means that encryption will not be built into most mass-market products. For example, it would make sense to build an encryption option into a standard e-mail program. But building encryption into an e-mail program would mean that the e-mail program could not be exported without a long, uncertain technical review. To avoid the technical review, companies are likely to leave out the encryption function. Network security will continue to suffer because encryption will not be built into mass-market products like e-mail or word processing programs.

Third, the requirement that encryption products be submitted for review before release violates the First Amendment. In April 2000 the Sixth Circuit Court of Appeals confirmed that encryption source code is speech protected by the First Amendment. The requirement that encryption products be reviewed before release is a "prior restraint" on speech.

Those problems with encryption export controls are widely recognized. The alternatives to the controls, however, have scarcely been examined, with the exception of "key escrow," or "key recovery." Development of encryption with key recovery features that guarantee the police access to the plaintext of a message must be rejected because

- introducing key recovery features may also introduce bugs and security holes in encryption products, like the holes discovered in recent versions of Pretty Good Privacy;

- developing key escrow for mass markets will for many purposes be technically impossible or very expensive;
- key escrow is incompatible with super-secure techniques such as ''perfect forward secrecy,'' or PFS, and many techniques for encrypting real-time communications;
- nonescrow encryption is widely available from foreign sources; and
- requiring secret keys to *ever* leave their users' secure environment endangers the security of the network.

Most important, it is wrong to bar anyone from using nonescrow encryption to communicate when he has done nothing wrong. Demands for mandatory key escrow constitute an unprecedented power grab on the part of law enforcement officials. The police have always had the right, limited by the Fourth Amendment, to intercept private communications and read them, *if they could*. The police have never had the right to demand that people change the language in which they communicate to make themselves easier to understand.

There are other alternatives to encryption regulations for law enforcement. They include increased use of informants and other surveillance technologies such as the planting of physical bugs or devices such as Tempest, which enables law enforcement to read the screen of a computer through walls or doors (of course, law enforcement officials must first have a warrant).

Encryption export controls should be lifted without qualification.

CALEA and the Expansion of Wiretapping

The pernicious principle that private businesses must rebuild their networks to help the police is embodied in the Communications Assistance for Law Enforcement Act of 1994 (CALEA). That law should be repealed.

The Federal Bureau of Investigation began to lobby for CALEA in the early 1990s, as phone companies began to deploy digital technology. In passing CALEA, Congress unconstitutionally delegated to the FBI a role in shaping the standards that telephone companies must meet to make their phone networks more amenable to wiretapping. Predictably, the FBI has since demanded far more power than the statute was intended to give it.

In particular, FBI director Louis Freeh testified before Congress in 1994 that, for wireless phone calls, CALEA would require phone companies to provide only the area code from which the person was calling, stating that in demanding CALEA the FBI had "no intent whatsoever . . . to

acquire anything that could properly be called 'tracking' information." Later, however, the FBI demanded that phone companies provide the exact location of the origination of a wireless phone call, allowing them to pinpoint the caller on a map.

In August 2000 a unanimous panel of the Federal Court of Appeals for the District of Columbia ruled that FBI demands for added surveillance features under CALEA went too far. The FBI had sought to be able to track any digits dialed during a call, such as bank account and credit card numbers. The court upheld the FBI's request to obtain information about the location of the antenna that was used to place a wireless phone call but rejected the idea that the FBI should be allowed to require telephone companies to triangulate the exact location of a wireless phone user.

However, the court failed to recognize that the U.S. Constitution was never intended to give the federal government—particularly the federal police—the power to dictate how phone networks would be constructed. A law like CALEA and the demands the FBI has made under it have no place in a free society.

Carnivore and Other Blanket Surveillance

An estimated 6 trillion e-mail messages pass through servers in the United States each year. People believe and expect that their e-mail is private and secure. But a threat to their privacy exists in the FBI's Carnivore system, which has the ability to invade and capture any e-mail. Preventing crime is a valid concern, but it is not necessary or right to subject the innocent and suspects alike to a massive system of surveillance. If the FBI has nothing to hide regarding Carnivore, why are they afraid to open Carnivore to public review by nongovernmental computer security experts?

- Carnivore is a security risk. Internet service providers (ISPs) have no say in the development or the installation of Carnivore. Carnivore is hooked into the ISPs' networks without any guarantee that it will not cause security breaches. The ISPs must rely on the FBI's own self-interested assertions of security.
- Less-intrusive means are available. Under current law, the FBI may require ISPs to turn over the correspondence of a suspect in a timely, accurate, and efficient manner. This system works efficiently, as demonstrated in a beta test by Peter William Sachs, head of ICONN, an ISP.

- An independent audit is essential to maintain trust. Questions remain about whether Carnivore monitors all logins to find the one it is searching for or whether it checks each message—both arguably illegal violations of the privacy of nontargeted individuals. To reassure the public, outside nongovernmental experts must examine the source code of the system during installation and monitoring. Internal review of Carnivore by the FBI will not satisfy the concerns of civil liberties groups, Congress, or private citizens. Both the selection of the auditor and the actual audit should be conducted with due diligence to answer questions about Carnivore in a timely manner. The auditors should report to Congress, not to the FBI.
- The risk of abuse is enormous. Tom Perrine of the San Diego Supercomputer Center says that "the ultimate concern of citizens should be the possibility of 'mass monitoring' of all the users at an ISP, a company, a university, or a state or a country." Carnivore is merely a tool; there is nothing to stop an agent from using Carnivore to gather all the network traffic he can gather and store—not simply that which his warrant authorizes.
- The FBI has historically abused its surveillance rights. Examples include the Church Committee investigations of the 1970s and electronic surveillance of Dr. Martin Luther King, Jr., dissident groups, and journalists. The most recent scandal involved the mysterious trip of 1,000 FBI files to the White House.
- The use of Carnivore without legislative approval or debate shows that the FBI gives short shrift to privacy concerns. Carnivore has existed for more than three years and has been installed in ISPs 25 times, including 16 this year. The law enforcement officials questioned have declined to provide specific details about the cases.
- Pending review, Congress should consider a moratorium on Carnivore's use. The FBI's current use of Carnivore may be illegal under the existing pen register and trap and trace statutes, and raises difficult constitutional issues.

Suggested Readings

Global Internet Liberty Campaign. "Cryptography and Liberty 2000: An International Survey of Encryption Policy." Washington, February 2000.

Matlick, Justin. "U.S. Encryption Policy: A Free-Market Primer." San Francisco: Pacific Research Institute for Public Policy, May 1998.

National Research Council. *Cryptography's Role in Securing the Information Society.* Washington: National Academy Press, 1996.

Reinhold, Arnold G. "Strong Cryptography: The Global Tide of Change." Cato Institute Briefing Paper no. 51, September 17, 1999.

Singleton, Solveig. "Encryption Policy for the 21st Century: A Future without Government-Prescribed Key Recovery." Cato Institute Policy Analysis no. 325, November 19, 1998.

Wolfe, Henry B. "The Myth of the Superiority of American Cryptographic Systems." Cato Institute Briefing Paper no. 42, November 12, 1998.

—Prepared by Solveig Singleton