19. Encryption and Wiretapping

Congress should

- lift all export controls on 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; and
- repeal the Communications Assistance for Law Enforcement Act, which treats every U.S. citizen like a suspect and phones as tracking devices.

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. At present, U.S. law restricts the export of any key length over 56 bits, to be reduced to 40 bits in January 1999. Stronger 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.

It is well known that export controls interfere with the marketing and sale of powerful encryption technology, imposing tremendous costs on

software and hardware developers. The controls are futile, easily evaded by smugglers. And the controls have been a tremendous boon to encryption innovators in other countries such as Ireland, Finland, New Zealand, and the United Kingdom. The longer the controls remain in place, the more capital and jobs will flee overseas.

In the end, the attempt to restrict cryptography will backfire, for U.S. law enforcement officers can expect little aid with decryption from security firms located in Finland or South Africa. And restricting the mass of users to keys of short bit length makes networks insecure; if a code can be broken by law enforcement, it can be broken by hackers.

Also, export controls violate the First Amendment. Those controls sometimes require academic research papers, clearly protected by the First Amendment, that discuss ideas about cryptography to be submitted to the government for review. And, as one court recently held, software expresses ideas in language and is also protected by the First Amendment. No other holding would have made sense; source code printed in a book is clearly protected by the First Amendment—the same source code stored on a computer disk should be equally protected. Because of export controls, some professors refuse to allow foreign students to take their classes, fearing reprisals from Commerce Department enforcers.

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

- 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.

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 only require phone companies to provide 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.'' Today, however, the FBI demands that phone companies provide the exact location of the origination of a wireless phone call, allowing them to pinpoint the caller on a map.

A law like CALEA and the demands the FBI has made under it have no place in a free society. The Constitution does not empower Congress to delegate to federal police the power to demand that surveillance devices be built into private communications networks.

Suggested Readings

Global Internet Liberty Campaign. ''Cryptography and Liberty: An International Survey of Encryption Policy.'' GILC, Washington, February 1998.

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

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

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 Superiority of American Encryption Products.'' Cato Institute Briefing Paper no. 42, November 12, 1998.

—Prepared by Solveig Singleton