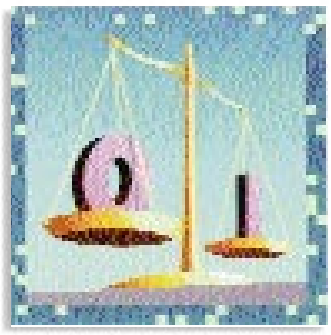
Strong Crypto, Weak Liberties



The U.S. Government is bugged, so to speak, about the future of wiretapping.

The Federal Bureau of Investigation (FBI) and the National Security Agency (NSA) have been agitated for years that developments in digital communications and cryptography will close the door on the era when it was easy for them to listen in on communications. Thus, they have urged Congress and the executive branch to mount a three-pronged attack by restricting public use of cryptography, asking manufacturers voluntarily to insert a "back door" in telecommunications devices, and requiring a similar back door in the national telephone network.

As has been reported periodically in this magazine, cryptography programs such as Phil Zimmermann's nearly unbreakable free software Pretty Good Privacy (PGP) have been classified as "munitions" under federal export laws. Until January, when all charges against him were dropped, Zimmermann, a consultant in Boulder, CO, had been under investigation by a federal grand jury for almost two years because someone posted PGP to the Internet, where it was downloaded by overseas users; this constitutes an illegal munitions export in the government's view. Zimmermann says, "I think this raises First Amendment issues, because the only way to comply with the law is not to publish at all."

Meanwhile, U.S. software companies are unable to compete in foreign markets with companies that offer much stronger encryption solutions in their products. Sun Microsystems has taken to incorporating encryption utilities developed abroad in products it manufactures overseas. Because no U.S. export is involved, Sun avoids Zimmermann's legal problems.

The feds also have been pushing various versions of the Clipper chip. Installed voluntarily by manufacturers of telecommunications devices, the chip would include software which would automatically transmit a copy of the key to any encrypted communication to the government. The key would be split into two parts, one of which would be held by the Treasury Department and the other half by the National Institute for Standards and Technology (NIST). The FBI would have to obtain a warrant from a federal judge in order to reunite the two halves of the key and "unlock" a suspect's communications.

However, both of the escrow agencies are part of the executive branch, as is the FBI, and many civil libertarians believe that abuse—deencryption of communications without a warrant—is likely. John Perry Barlow, cofounder of the Electronic Frontier Foundation, says, "Trusting the government with your privacy is like trusting a Peeping Tom with your window blinds." So far, the Clipper chip has won little support from the manufacturers whom the feds hope will support it.

A Mandate to Eavesdrop

Not content to have a back door into the devices that originate communications, the government also wants to build its monitoring capability into the network itself. In the past, monitoring of phone calls has involved attaching a device to the wire; the Digital Telephony Act, passed at the end of last year's congressional session, awaits funding by this congress. This act would effectively permit the FBI to flip a switch to listen to any telephone call. Although warrants would still be required, the possibilities for abuse are significant.

Last year, federal courts authorized fewer than 1,000 wiretaps nationwide, and the FBI has not claimed that any of these investigations were thwarted by encryption or the need to use traditional means of eavesdropping. The FBI's proposed implementation of the system called for by the Digital Telephony Act would cost $500 million and would give the agency the capability to monitor one out of every 1,000 phone lines (in certain parts of the country, listening in on as many as one of every 100 phone calls). Obviously, since many millions of phone calls are made in this country every day, the FBI's new wiretap capability will far exceed the 1,000 wiretaps it actually performed last year.

Prophets of "technological determinism" agree that human beings want to use new toys to the full extent of their capability. It can be expected that if Congress funds the Telephony Act, we will see a lot more wiretapping.

When new technology is involved, fear, uncertainty and doubt always seem to cloud the issue and keep policymakers and the public from spotting simple

By Jonathan Wallace

parallels. It took the Supreme Court 50 years to recognize that a movie is protected by the First Amendment just like a play or a novel. In the 1980s, courts were confused whether software, which was recognized to be copyrightable if stored on disk, was protected if stored in ROM. The analogy that many don't see in the debate on wiretapping and civil liberties is that it is as if the government is actually asking you to deposit a copy of the key to your house. These federal agencies want to be able to come in and take a look around whenever they want, but they promise they will get a warrant first. Can they be relied on to keep that promise?

The debate about cryptography is prejudiced by a perception that honest people don't need to encrypt communications. But the very reason that U.S. companies are losing market share in Europe is that businesspeople do, in fact, want to encrypt sensitive data and communications before sending them out over an insecure wire. We all have that same right. Phil Zimmermann says, "I should be able to speak to you in Navajo if I wanted, even if law enforcement can't understand Navajo." The ban on secure cryptography is analogous to the government telling you you must speak in loud, clear English in your living room, so it can eavesdrop better.

The FBI isn't looking too good to congress and the public in the aftermath of the shoot-outs at Waco and Ruby Ridge. This situation currently provides the main hope that congress will not reach into the public purse for the required $500 million to build the FBI's back door into the national telephone system. IT

Jonathan Wallace *is vice president and general counsel of Pencom Systems, Inc., in New York City. He can be reached at jw@pencom.com. His colleague Mark Mangan provided research for this article.*

ADVERTISING INDEX

World Wide Web addresses of *UniForum's IT Solutions* advertisers are listed complimentarily each month.

ADVERTISING SALES OFFICES

Northwestern U.S. and Western Canada
Charles Abrams (415) 621-6700
Charles Abrams and Associates (415) 621-6760 fax
24 Ford St.
San Francisco, CA 94114

Southwestern U.S.
Pat Macsata (510) 888-1104
R.W. Walker Co. (510) 888-0472 fax
22971 Sutro St., Ste. B
Hayward, CA 94541

Midwestern U.S. and Central Canada
Thomas Fitzpatrick (708) 653-1611
TF Marketing Associates (708) 653-1612 fax
1496 County Farm Ct.
Wheaton, IL 60187

New England and Eastern Canada
Mark Schelling (617) 769-8950
Hajar Associates (617) 769-8982 fax
49 Walpole St.
Norwood, MA 02062

Mid-Atlantic U.S.
Barbara Best (908) 741-7744
Hajar Associates (908) 741-6823 fax
569 River Rd.
Fair Haven, NJ 07704

Southeastern U.S.
Scott Rickles (770) 664-4567
Ray Rickles & Co. (770) 740-1399 fax
560 Jacaranda Ct.
Alpharetta, GA 30202

Europe
Huson European Media
Gerald Rhoades-Brown 01784-469900
10/11 The Green Business Centre 01784-469996 fax
The Causeway, Staines
Middlesex, TW18 3AL, United Kingdom

Publisher's Sales Office
Richard Shippee (408) 986-8840, x17
UniForum's IT Solutions (408) 986-1645 fax
2901 Tasman Dr., #205 e-mail:
Santa Clara, CA 95054 dick@uniforum.org