British MI5 to gain access to encryption keys

Mike Ingram
6 May 1998

The British Labour government has proposed the introduction of new legislation that represents a major infringement on communications privacy.

Two new laws are to be drafted by the Home Office enabling intelligence and law enforcement agencies to obtain a warrant for access to information necessary to decrypt the contents of communications or stored data delivered by e-mail. Failure to hand over the information will be deemed a criminal offence.

The plan was justified in Parliament last week by Trade and Industry Minister Barbara Roche as a means of combating money laundering, terrorism and international criminal organisations.

The issue of encryption technology has been the subject of intense discussion in state departments throughout the world. In Britain and the US, export controls have been used as a way of preventing the distribution of strong encryption systems, unless the relevant national intelligence agencies were able to read the codes.

Companies such as Microsoft, Lotus and Netscape have complied by distributing weakened versions of their built-in encryption systems to non-US customers. Others have used the First Amendment of the US constitution—which prohibits restrictions on free speech—to refuse to comply with government and FBI demands.

Phil Zimmermann recently received the Lifetime Achievement Award for his Pretty Good Privacy (PGP) public key encryption software. He repeatedly refused to comply with US federal government demands that he allow security forces a "back door" to read files and messages encrypted with his software. Recently the last two versions of PGP were legally exported from the US in the form of huge textbooks of code, which were then scanned in and recompiled in electronic form by a team of researchers in Europe.

In an attempt to calm widespread fears of an infringement on democratic rights, the British government says that users and providers of encryption software will have to hand over codes "only when appropriate authority has been obtained—for example, a judicial warrant."

These statements have been greeted with widespread scepticism. Leading civil rights lawyer Geoffrey Robertson QC told the *Guardian* newspaper: "This would be a monumental advance on government's rights to invade privacy.... A judicial warrant can come from a lay justice or a circuit judge whom the police select. It's a classic case of Neanderthal thinking—no safeguard at all."

"Do they really think that major criminals go home and log their crimes on the Internet in a computer diary?" Robertson asked.

Last week's announcement was made after three months of deliberation by the Prime Minister's policy unit. Alongside the Home Office plans, the Department of Trade and Industry is to draft a new law regarding electronic commerce.

New Labour's original plan was to adopt the so-called "key escrow" system put forward by the previous Tory government. In March 1997, the Major government issued a proposal for "Licensing of Trusted Third Parties for the Provision of Encryption Services." They planned for privacy keys to be held compulsorily in central data banks, where police or intelligence agencies could electronically retrieve them if they wanted to read particular communications.

This system was condemned as complex, costly, dangerous and unworkable. The European commission said last October that such central key recovery systems created enormous security dangers as well as significant cost for the user, yet provided no real benefit in dealing with terrorism or major crime.

The new law proposed by the Department of Trade and Industry appears to address some of these issues. A licensing system for "Certification Authorities" will be set up. Licenses will not be compulsory, but these will be the only digital signatures to be legally recognised, thus making it a de-facto standard.

The Government claims that the purpose of the plan is "to offer certificates to support electronic signatures reliable enough to be recognised as equivalent to written signatures." The main use of digital signatures is to verify

the identity of customers who place orders for goods or services electronically, which are then often delivered electronically. This type of trade is expected to be worth £5 billion a year in Europe alone.

In announcing the two new laws, however, Roche made an explicit link between digital signatures and demands for key recovery systems. Licensed service providers that offer encryption services will be required to make the recovery of keys possible through suitable storage arrangements.

The announced legislation is an attack on democratic rights. Predicting technical difficulties with the new laws, legal experts have pointed out that if the only suspected evidence of a crime is the unknown contents of encrypted files on a computer, forcing a user to unlock them by handing over codes would effectively remove the right to silence.

The routine use of telephone bugging and mail interception has been well documented not only in criminal cases but in the targeting of political and civil rights activists. The expansion of these practices into the field electronic data should be of concern to anyone who believes in civil liberties.

One of the great attractions of the Internet and electronic communications in general is the possibility opened up for people to communicate on a far greater scale than ever before. Never has the opportunity for individuals or organisations to make their views known to a world audience been so readily available.

Far from welcoming such an interaction of ideas, in electronic communications as in other walks of life, the powers-that-be fear nothing more than a free and democratic discussion on the society in which we live and the possibility for change. This is the real reason behind the campaign for state monitoring of electronic data and censorship of the Internet.