Crypto Controls are Spreading Internationally

Hand over that encryption key, mate, monsieur, sir, bloke.

By David Banisar Jul 15, 2002

Five years ago, when the Organization for Economic Cooperation and Development (OECD) released their guidelines for cryptography policy, crypto advocates cheered and declared victory. After a hard fought battle, we had forced the OECD to back away from the U.S. government's efforts to restrict encryption worldwide. After the guidelines, countries around the world issued crypto policies that called for the free and unfettered use of encryption products to promote e-commerce and protect privacy. Eventually, even the U.S. gave up anddropped most export controls. In the last EPIC Cryptography and Privacy survey, written in 2000, there were only a handful of nations that still restricted crypto, like Burma, Belarus, and Russia -- countries you really didn't want to go to anyway.

We expected a golden era of privacy and security, with encryption allowing us to protect our computers and communications from attacks, make purchases with digital cash, and anonymously browse the net. Once crypto was out in the world it would become ubiquitous and could never be restricted again. We even got complacent. We moved onto new battles.

It's time to wake up again. Worldwide, there is now a movement back towards restrictions in the name of fighting cybercrime and terrorism. And we are losing again.

The trend started before September 11. In the U.K., the Regulation of Investigatory Powers (RIP) Act allows police, tax collectors and others to imprison for two years users who refuse to hand over the plaintext of communications, or the keys to unlock them. The government hasn't figured out how to manage the details, so the RIP Act is not yet in force, but given that the government recently attempted to extend the act to allow Internet surveillance by postal workers and the local town councilors, it seems likely that when they do implement it, it will be in the worst possible way. Virtually none of the cryptographic killer apps we fought for are actually being used.

Similarly, the Council of Europe (COE) cybercrime convention requires countries that sign on to enact laws allowing police to demand keys in the name of providing international assistance. In December 2001, the Australian government enacted a new law on cybercrime that includes the ability to throw users in jail who don't give up their keys. Attorney General Daryl Williams said that Australia was required by the COE convention to adopt the provision -- a disingenuous claim, since they are not a signatory and are not bound by the treaty. The New Zealand Law Commission considered doing the same, but decided to only require that third parties assist in decryption efforts, due to concerns over forcing suspects to incriminate themselves.

It's a Small World After All

In France, advocates cheered in 1999 when the French government dismantled what the NSA described (perhaps admiringly) as "the most comprehensive cryptologic control and use regime in Europe, and possibly worldwide." Three years later, the Parliament approved the "Loi sur la Sécurité Quotidienne" (LSQ) that requires users to give up their keys, or face three years in prison. Mon Dieu!

In South Africa, the fear of crime, wielded deftly by an increasingly repressive government, is steering the democratic system down the road of its totalitarian predecessor. A new Electronic Communications and Transactions bill recently passed in the parliament and is awaiting the president's signature. It would require that all providers of encryption services operating in South Africa register with the government. A "cyber-inspector" corps would be set up to investigate and ensure compliance.

Not to be outdone, the Netherlands -- liberal by reputation, but with over 10,000 wiretaps a year quite aggressive in domestic spying -- is even discussing key escrow again. They would require trusted third parties to house copies of every encryption key used by anyone. It doesn't seem to matter to them that the concept was thoroughly discredited years ago by the rest of the world.

Meanwhile, virtually none of the cryptographic killer apps we fought for are being used.

DigiCash is gone, PGP has been orphaned, and ZKS dropped Freedom and is selling consulting services to stay alive. Not exactly a golden era.

About the only country where it seems safe to use crypto is the U.S. After years of being caned by industry and privacy groups to relax export rules and ignore the FBI's push for crypto controls, the bureaucrats and politicians must have learned this was a no-win situation. So when Senator Judd Gregg (R-NH) reacted to September 11 by suggesting that all crypto without backdoors be banned, the howls were strong for him to drop the plan within weeks, and nothing was included in the USA Patriot Act.

This shows that vigilance is still important in the U.S. But we can't afford to be complacent internationally either. If the rest of the world adopts restrictions, we will once again be facing the argument that America must restrict crypto, because everyone else is doing so. It we don't use it, we will lose it.

David Banisar is a research fellow at the Harvard Information Infrastructure Project at the Kennedy School of Government at Harvard University and Deputy-Director of Privacy International.