FORTUNE

Apple and the FBI re-enact the '90s Crypto Wars

by Philip Elmer-DeWitt

September 27, 2014

The privacy features on Apple's new iPhones have got the three-letter agencies spooked.

I was reminded last week of a story that broke in the early-1990s, while I was covering tech for Time Magazine. The Department of Justice had targeted a programmer named Phil Zimmermann whose crime — as the government saw it — was writing an application called Pretty Good Privacy and releasing it on the Internet.

Zimmermann, as I recall, nearly went to jail.

PGP was strong crypto, strong enough to be classified as a munition and subject to the Arms Export Control Act.

It wasn't invincible — no crypto scheme can resist forever a supercomputer with enough time to try every permutation of letters, numbers and punctuation marks. But Zimmermann's program was the first popular application of an asymmetric technology called public key encryption that made secret codes harder — by many factors of ten — for even the NSA's computers to crack.

The U.S. government eventually lost the Crypto Wars, as Wired dubbed them. Zimmermann went free, and law-abiding U.S. citizens today can protect everything from Facebook passwords to Caymen Island bank accounts with public key encryption.

I was reminded of all this last week when Apple found itself at the center of another crypto blow up, this one led by FBI director James Comey and fought on the op ed pages by retired FBI agents and the libertarians of the Cato Institute.

At issue are the privacy features with which Apple equipped its new iPhones, from TouchID fingerprint readers to hardwired Secure Elements, where passwords and credit numbers are assigned unique identifiers and locked under double key.

"If the government laid a subpoena to get iMessages," Apple CEO Tim Cook told Charlie Rose on national TV last week, "we can't provide it. It's encrypted and we don't have a key."
Cooks remarks did not please certain subpoena-issuing government agencies.

“What concerns me,” FBI director Comey said Thursday at a press conference devoted largely to combatting ISIS terrorism, “is companies marketing something expressly to allow people to hold themselves beyond the law.”

He went on, according to the New York Times’ David Sanger and Brian Chen, to evoke every parent’s worst nightmare:

He cited kidnapping cases, in which exploiting the contents of a seized phone could lead to finding a victim, and predicted there would be moments when parents would come to him ‘with tears in their eyes, look at me and say, What do you mean you can’t’ decode the contents of a phone.
“The notion that someone would market a closet that could never be opened — even if it involves a case involving a child kidnapper and a court order — to me does not make any sense.”
The ironies here are thick.

On one hand, Apple brought this on itself, using crypto as a marketing tool to sell more iPhones.

On the other, Apple might not have gone down this road if Edward Snowden hadn’t blown the whistle on the NSA’s domestic surveillance programs — including, according to one NSA slide, a secret back door into Apple’s servers.

In the end, it’s not clear that the government’s ability to track down kidnappers — or terrorists, for that matter — will be greatly hampered by Apple’s Secure Elements. They only limit access to contacts and other data stored on the phone itself. They don’t make it any harder to legally intercept phone calls or e-mail.

“Eliminating the iPhone as one source I don’t think is going to wreck a lot of cases,” security expert Jonathan Zdziarski told the Times. Investigators, he said, have “a mountain of other evidence from call logs, e-mail logs, iCloud, Gmail logs. They’re tapping the whole Internet.”