

The Forced Disclosure of Encrypted Data

Christopher Soghoian

Information Security Institute

Johns Hopkins University

April 21 2004

The Moral and Legal Foundations of Privacy

Professor Andrew W. Siegel

"Uncrackable encryption is allowing terrorists — Hamas, Hezbollah, al-Qaida and others — to communicate about their criminal intentions without fear of outside intrusion ... they're thwarting the efforts of law enforcement to detect, prevent and investigate illegal activities."

FBI Director Louis Freeh during closed-door testimony on terrorism before a Senate panel, March 2000.

The Use of Encryption by Terrorists

Khalil Deek, an alleged terrorist arrested in Pakistan in 1999, used encrypted files to store his plans for a bomb attack in Jordan. His computer was flown to the National Security Agency, which was able to decode the files. This enabled the FBI to foil the plot.ⁱ

Ramzi Yousef, the convicted mastermind of the World Trade Center bombing in 1993, used encrypted files to hide details of a plot to destroy 11 U.S. airliners. Law enforcement officials broke the encryption and foiled the plot. It reportedly took two years for the FBI to decrypt two of his files.

Kevin Mitnick was the first hacker to appear on the FBI's most wanted list. His exploits include breaking into the computers of NORAD, the California DMV and Digital Equipment Corporation. A fugitive for two and a half years, he was finally arrested by the FBI in 1995. He was held in jail, at times in solitary confinementⁱⁱ, for over four years without trial before finally pleading guilty to computer-related crimes.

Authorities seized two of Mitnick's laptops during his arrest. Over a gigabyte of encrypted data was held on his laptops, secured with a key that Mitnick refused to reveal.ⁱⁱⁱ Under Rule 16 of the Federal Rules of Criminal Procedure, the government must allow a defendant to inspect or copy documents that "were obtained from or belong to the defendant." Mitnick's lawyers hoped to use his encrypted data to help build a defense case. The prosecution objected and said the situation was akin to Mitnick asking for his coat back and the government not knowing if there was a pistol in the pocket. Judge Pfaelzer agreed, ruling that "this court is not going to order the encryptive [sic] material to be given" to Mitnick.

When the government comes across encrypted data in the course of an investigation, they are presented with several options that force them to choose between prosecuting that individual and having access to the encrypted data:

1. They can send the encrypted data to the NSA for brute-force decryption.

However, one wonders why the government was able to crack the encryption used by two terrorists in time to foil their plots, but was not able to decrypt Mitnick's data during the four years he was held in jail. One would presume that a hacker who gained access to NORAD's networks would pose enough of a threat to warrant the NSA's involvement.

2. They can offer immunity to the suspect. Once given immunity, the defendant loses 5th Amendment protections against self-incrimination and can then be forced by a judge to disclose the keys to the encrypted data.
3. They can attempt to build a case against him without the encrypted data, and deny him access to that data for his defense case.

Lawful Access and Forced Disclosure of Encryption Keys

*“Note that a court could cite you for contempt for not complying with a subpoena duces tecum (a subpoena requiring you to produce objects or documents) if you fail to turn over subpoenaed backups....To be honest, I don't think *any* security measure is adequate against a government that's determined to overreach its authority and its citizens' rights, but crypto comes close.”^{iv}*

Mike Godwin, Electronic Frontier Foundation Legal Council,
June 1993.

In the previously described cases, the government was either able to crack the file encryption, or it had a sufficiently strong case that enabled them to prosecute the defendant without access to the encrypted data.

In *Doe v United States*, 487 US 201, 219 (1988), Justice Stevens wrote in dissent, “[a defendant] may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe--by word or deed.”

This seems to suggest that the only way the government can force access to a defendant’s encrypted data is to offer him some kind of immunity deal. However, if the information contained in the encrypted files were about a third party, and not the holder of the encryption keys, the government could easily force their disclosure. This is very similar to the situation that journalists find themselves in when they are forced to disclose

their sources by a court. As they do not risk self-incrimination by the disclosure of that data, they have no legal grounds to withhold it.

Responses to an Order to Disclose Encryption Keys

The only available responses to a government order to disclose encryption keys appear to be:

1. “I don’t know the key. The data is not mine”
2. “I’ve forgotten the key.”
3. “I refuse to tell you.”

The first choice could be quite difficult to prove, especially if the encrypted data was on the defendant’s computer amongst his other files.

The second choice is a gamble. If he can convince the judge that he has honestly forgotten the key (i.e. the file is several years old, and seldom decrypted), it is possible that he could escape without prosecution.

If either the judge didn’t believe the defendant’s answer in the first two choices, or he chose the third, then it is highly likely that he would face some kind of contempt of court charge, and thus jail time. Again, this is similar to journalists who refuse to give up their sources, and whom the courts have historically shown little lenience to.^v

Key Escrow

"Between 1993 and 1997 police representatives were not involved in the NSA [National Security Agency]-led policy-making process for key recovery. Despite this, during the same period the U.S. government repeatedly presented its policy as being motivated by the stated needs of law-enforcement agencies."^{vi}

A 1999 Scientific and Technological Options Assessment panel report to the European Parliament

"Police forces are reluctant to use "escrowed" encryption products (such as radios in patrol cars). They are more costly and less efficient than non-escrowed products. There can be long gaps in reception due to the escrow features -- sometimes as long as a ten second pause. Our own police do not use recoverable encryption products; they buy the same non-escrowable products used by their counterparts in Europe and Japan."^{vii}

A November 1996 Memo written by William A. Reinsch, the Commerce Department's Under Secretary for Export Administration

In the early nineties, the so-called 'crypto wars' were fought between cypherpunks (cryptography activists) and the government. Secure and unbreakable encryption software such as Pretty Good Privacy, written by MIT's Phil Zimmermann, had been anonymously released to the Internet at large, in spite of the government's requirement that strong cryptographic software not be made available for export.^{viii}

At the same time, the Clinton administration pushed for the use of ‘key escrow’ technologies, and specifically of the Clipper Chip. This NSA-developed cryptographic device encrypted data with two separate keys: one for the user, and one held by the government so that a user’s data could be accessed at a later date by law enforcement.

The government assured critics that the escrowed keys would only be revealed after search warrant had been issued. However, the proverbial cat of strong encryption was already out of the bag. Academics were releasing new escrow-free encryption schemes, and foreign companies were taking full advantage of the strong-crypto export prohibition to sell their products in world markets where US companies were unable to compete. Users saw little reason to use expensive and untrustworthy escrow systems when secure and backdoor-free products were available for free on the Internet or commercially abroad.

In 1998, Matt Blaze, a security researcher at AT&T Labs published a critical flaw in the Clipper system^{ix}. The following year, the Clinton administration announced it was voluntarily lifting the export restrictions on encryption products to all but 7 terrorist-supporting nations.^x These two events seemed to bury the key escrow issue once and for all.

While key escrow would seem to solve the tricky problem that encryption technologies present to the government, it is clearly not a realistic solution. The only way to force its widespread use would be to ban the use of cryptographic software lacking the government backdoor – which would be exceedingly difficult regardless of the questionable constitutionality of such an action.

Conclusion

The issue of encryption is one that draws strong opinions from both sides. Cypherpunks and cyber liberty activists completely reject any attempt by the government to limit their use of encryption technologies, whereas elements within the government wish to completely ban the use of strong encryption, and force the use of so called key escrow services.

The use of encryption technologies, by both the good guys and the bad, is on the rise. Perhaps the NSA will be able to continue to decrypt files at will, but the Mitnick case seems to suggest that this is not possible in all situations. It is therefore likely that we will see the government resorting to alternate means to discover the contents of encrypted files.

The government will find itself in the difficult situation of deciding between offering suspects immunity for their files, or forgoing access to potentially critical evidence and intelligence. Individuals too will find themselves in an interesting situation, as they will increasingly be given the tough choice between disclosing their secrets and spending time in jail.

There is a significant lack of case law in the areas surrounding encrypted data. Thus, this promises to be an interesting chapter in the on-going privacy wars as the government struggles to deal with the changes that encryption and other 'disruptive technologies' bring to the legal battlefield.

References

- ⁱ Terror groups hide behind web encryption, USA Today,
<http://www.usatoday.com/tech/news/2001-02-05-binladen.htm>
- ⁱⁱ Mitnick Lands in Solitary, Wired News,
<http://www.wired.com/news/business/0,1367,1715,00.html>
- ⁱⁱⁱ Wrinkle in Mitnick Case Hints at Encryption Battles to Come, NY Times Cyber Law Journal, <http://nytimes.com/library/tech/00/01/cyber/cyberlaw/28law.html>
- ^{iv} Mike Godwin, Cypherpunks email list posting,
<http://cypherpunks.venona.com/date/1993/06/msg00429.html>
- ^v Nation Magazine, A Tale of Two Journalists,
<http://www.thenation.com/outrage/index.mhtml?pid=1002>
- ^{vi} Report: US uses Key Escrow to Steal Secrets, TechWeb Magazine,
<http://www.techweb.com/wire/story/TWB19990518S0004>
- ^{vii} Key Escrow, Electronic Privacy Information Center,
http://www.epic.org/crypto/key_escrow/
- ^{viii} Why I wrote PGP, Phil Zimmermann,
<http://www.philzimmermann.com/EN/essays/index.html>
- ^{ix} Clipping Clipper: Matt Blaze, Wired News,
<http://www.wired.com/wired/archive/2.09/eword.html?pg=7>
- ^x US Attorney General nominee is pro-privacy, The Register,
http://www.theregister.co.uk/2001/01/04/us_attorney_general_nominee/