

**Christopher Soghoian**

**The Privacy Wars: Widespread Encryption for All**

**Law and Policy of Information Assurance**

**Prof. Darren Lacey**

**Johns Hopkins University**

**Information Security Institute**

**March 29 2004**

For many years, cypherpunks<sup>1</sup> and privacy activists have been encouraging the population to encrypt all of their traffic<sup>2</sup>. There are multiple reasons for this:

Many believe that the NSA has the capacity to crack existing consumer encryption technologies. Even though the agency famously<sup>3</sup> measures its computing power in acres, they still have a finite amount of computing power, as proven by their failure<sup>4</sup> to translate 9/11 intercepts in time.

The NSA and other agencies, using such systems as Carnivore<sup>5</sup>, are already running pattern matches on captured data (phone, email, etc). Given that the vast majority of email and instant messenger traffic sent today is sent unencrypted, it is quite feasible for the NSA to concentrate their resources on this traffic.

Were everyone to use encryption, even if just for their sensitive messages, it is quite possible that the NSA would run out of resources. Some believe this is one of the reasons for the government's position during the crypto-wars. According to the theory, the government did not care so much about encryption software being released, because it is always assumed that smart criminals, foreign governments and academic researchers have access to such technologies. However, the government wishes to avoid at all costs the widespread adoption of easy to use encryption technology. This would create such a flood of data that they'd have no idea what to concentrate their attention and presumably limited resources on.

If every individual uses encryption solely for his sensitive communications, it is possible for the government to perform traffic analysis upon them. If a sudden burst of encrypted communications from one person to another was observed, it would be quite reasonable to assume that something important was happening. Once the public at large

starts using encryption for all traffic, sensitive or not, it becomes impossible for the NSA to target individual communications for analysis, and for them to guess any information through traffic analysis techniques.

“I’m not doing anything illegal, so why should I care?”

-- Joe Sixpack.

Even though U.S. citizens may be willing to overlook their government’s misdeeds in the past, there are several reasons for them to be concerned about their exposure to government/private prying eyes.

Many foreign governments snoop on electronic data. While a person may happily trust his own government to respect his privacy, should he trust every other foreign government out there to respect his privacy too? Anti-U.S. feeling is quite strong in many countries, and so their citizens will probably want to protect themselves against NSA-lead privacy attacks.

In addition to the much-hyped Carnivore surveillance system, the United States and other Anglo countries participate in a information-sharing system known as ECHELON. This system has reportedly tapped the communications of private companies, individuals, and even charities such as Amnesty International and Christian Aid.

In 1999, The House Select Committee on Intelligence began to look into the legal basis for the NSA's ECHELON activities. In particular, the Committee wanted to know if the communications of Americans were being intercepted and under what authority, since

US law severely limits the ability of the intelligence agencies to engage in domestic surveillance. When asked about its legal authority, NSA invoked the attorney-client privilege and refused to disclose the legal standards by which ECHELON might have conducted its activities.<sup>6</sup>

Between 1956 and 1971, the FBI ran COINTELPRO, a program of surveillance and sabotage against political dissidents, thousands of whom, including Martin Luther King Jr. were innocent. In the early 70's, the program was exposed, and in response, reforms were put in place to prevent the government from spying on political groups when there was no suspicion of criminal activity.

Under the guise of the PATRIOT Act, it appears that the government again up to no good. In February 2004, federal authorities obtained a subpoena demanding that Drake University turn over records from an antiwar conference called "Stop the Occupation! Bring the Iowa Guard Home!" In March 2003, Members of the Aurora, Colorado Joint Terrorism Task Force infiltrated the Colorado Coalition Against the War in Iraq. They attended meetings, protests, and even got arrested with the other protestors as part of a non-violent trespass at a National Guard base.<sup>7</sup>

Given these government programs of snooping on citizens, charities and political groups, and in addition, the risks posed by rogue computer hackers and corporate interests, it seems very wise for users to employ widespread encryption for their data.

### **Encryption used by Terrorists and Criminals.**

*“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.

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 that was able to decode the files, thus enabling the FBI to foil the plot.<sup>8</sup>

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. U.S. officials broke the encryption and foiled the plot. It reportedly took two years for the FBI to decrypt two of his files.

Nicodemo Scarfo Jr, the son of a jailed Mafia boss was in 1999 arrested and charged with supervising a gambling operation. The detailed records of his business were kept encrypted on his computer, and it was only after the FBI covertly connected a keystroke recorder to his keyboard that they were able to decrypt the evidence they needed to prosecute him.

Clearly, there is a shady side to the encryption debate. For encryption technology to be made available to the public at large, it must also be made available to those who wish to do evil. However, we as a society have had to deal with the effects of so called

‘dual use technologies’ before: nuclear fission, guns and the sale of fertilizers containing ammonium nitrate.

The current RIAA and MPAA fueled lawsuits seem to be forcing users off insecure p2p networks, and are helping to encourage the rapid evolution of attack resistant anonymous networks. It is only a matter of time before every home computer with teenage users will be using high-end encryption technology for the exchange of files. As we have seen with previous technology rollouts (i.e. the web browser), once the foundations are in place, other technologies will appear that also use that functionality.

With any luck, the genie is already out, and widespread encryption will be the norm in a few short years. The overall effect this will have on society has yet to be seen, but I believe that the pros will far outweigh the cons. The government will find other ways to spy on people (and occasionally, criminals), but users will have won a crucial battle in the privacy wars.

---

## References

<sup>1</sup> The Jargon Dictionary: Cypherpunk,

<http://info.astrian.net/jargon/terms/c/cypherpunk.html>

<sup>2</sup> Use of encryption: not when its needed, <http://www.advogato.org/article/650.html>

<sup>3</sup> NSA and Information Processing Techniques at ARPA,

<http://www.sun.com/960710/feature3/sketchpad.html>

<sup>4</sup> Justice may probe leaked pre 9/11 intercepts,

<http://www.cnn.com/2002/US/06/20/911.warning/>

<sup>5</sup> Carnivore FOIA Documents,

[http://www.epic.org/privacy/carnivore/foia\\_documents.html](http://www.epic.org/privacy/carnivore/foia_documents.html)

<sup>6</sup> Echelon Watch, <http://archive.aclu.org/echelonwatch/faq.html#27>

<sup>7</sup> Outlawing Dissent, Salon.com,

<http://www.salon.com/news/feature/2004/02/11/cointelpro/index1.html>

<sup>8</sup> Terror groups hide behind web encryption, USA Today,

<http://www.usatoday.com/tech/news/2001-02-05-binladen.htm>