

CURRENT U.S. ENCRYPTION REGULATIONS: A FEDERAL LAW ENFORCEMENT PERSPECTIVE

*Charles Barry Smith**

Good afternoon. My name is Barry Smith, and I am a Supervisory Special Agent currently assigned to the FBI's Office of Public and Congressional Affairs as the Chief of that office's Digital Telephony and Encryption Policy Unit. For the past two and a half years, I have worked both on Capitol Hill and within the Clinton Administration to develop balanced encryption public policies.

Unfortunately, many people have drawn the false conclusion that restrictions on the export of encryption are newly evolved. The truth is that the United States, along with thirty-three other countries throughout the world, have been restricting the export of encryption for years.¹ Those restrictions have been in place to protect national security and foreign policy interests, not necessarily the interests of public safety and law enforcement.² I have purposely made a clear distinction there and I think you should as well.

* Supervisory Special Agent/Unit Chief of the Federal Bureau of Investigation's Digital Telephony and Encryption Policy Unit. What follows is a lightly revised version of oral remarks delivered at the New York University School of Law's Encryption Symposium.

1. See Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, July 12, 1996, *available in* <<http://www.wassenaar.org/docs/IE96.html>> [hereinafter Wassenaar Arrangement]; Wassenaar Arrangement, 15 C.F.R. § 743.1 (1999). The Wassenaar Arrangement was signed on July 12, 1996 and currently includes: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway, Poland, Portugal, Romania, Russia, Slovakia, South Korea, Spain, Sweden, Switzerland, Turkey, Ukraine, the United Kingdom, and the United States. *See id.* For a reference to current U.S. export regulations, see United States Export Administration Regulations, 15 C.F.R. §§ 730-774 (1998).

2. *See The Encryption Debate: Criminals, Terrorists, and the Security Needs of Business and Industry: Hearing on the Impact of Encryption Technology on Public Safety and Law Enforcement, Focusing on the Security Needs of Business and Industry and the Use of Encryption By Organized Crime and Terrorists Before the Subcomm. on Technology, Terrorism, and Government Information of the Senate Comm.*

Current export restrictions do not prevent you from exporting strong encryption; however, they do require that you not export strong encryption without a license from the government of one of these thirty-three countries. To obtain that license, the exporter must articulate what type of encryption technology is being exported, where it is being exported to, whether it is being sent to one of the seven terrorist countries, and in what way the encryption will be used once exported.³ With a license, you can export from the United States the strongest, most powerful encryption technology available. What you cannot do, however, is just export it to anybody anywhere, regardless of the consequences. So, let me make that really clear from the outset.

The introduction of digital technology and computer technology created an onslaught of encryption that is now publicly available for commercial and individual uses.⁴ Heretofore, the law enforcement community was generally not concerned about encryption, because that community had not been exposed to encryption technology to any degree. Nevertheless, encryption is now being used to protect all sorts of electronic communications, whether it be telephone calls, e-mail traffic, or stored data on your computers;⁵ and, that is just the beginning.

on the Judiciary, 105th Cong. 41 (1997) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (stating that in contrast to national security interests of controlling export of encryption, law enforcement “is more concerned about the significant and growing threat to public safety which could be caused by the proliferation and use *within* the United States of a communications infrastructure that supports the use of strong encryption”) (emphasis added) [hereinafter Freeh Testimony].

3. See Encryption Commodities and Software (ENC), 15 C.F.R. § 740.17 (1999); Encryption Items, 15 C.F.R. § 742.15 (1999). The seven terrorist countries include Cuba, Iran, Iraq, Libya, North Korea, Sudan, and Syria. See 15 C.F.R. § 740.17. The United States Department of Commerce Export Administration Regulations control the export of all encryption products except those encryption products specifically designed or modified for military use—which are regulated by the United States Department of State. See Exec. Order No. 13,026, 61 Fed. Reg. 58,767 (1996).

4. See AMITAI ETZIONI, *THE LIMITS OF PRIVACY* 75-76 (1999) (emphasizing increased demand for encryption from businesses using encryption to protect themselves against espionage by competitors and establishing secure links with partners, suppliers, and customers; bank and investment houses relying on encryption to ensure confidentiality of their transactions; and individuals using encryption to protect private communications). As of September 1997, one source had identified 1,601 encryption products manufactured and distributed by 941 companies in at least 68 countries. See *id.* at 76.

5. See FEDERAL BUREAU OF INVESTIGATION, U.S. DEP’T OF JUSTICE, *ENCRYPTION: IMPACT ON LAW ENFORCEMENT* 3 (1999) (reporting that encryption provides security for “conventional and cellular telephone conversations, facsimile transmissions, local and wide area networks, communications transmitted over the Internet (E-mail, etc.), personal computers, wireless communications systems, electronically stored informa-

We, in the law enforcement community—whether at the federal, state, or local level, think that is great. We support an encryption policy that allows users to have the strongest, most powerful encryption available to them to protect their private communications and their sensitive stored data. We support that. What we are concerned about, however, are criminals and terrorists that threaten public safety by using commercially available encryption products to prevent law enforcement from engaging, pursuant to the Fourth Amendment, in reasonable searches based on probable cause of criminal activity. We believe this represents a serious threat to public safety.

Unfortunately, there is a misconception within the general public that law enforcement agencies wiretap everyone's communications and read everyone's e-mail.⁶ This is just not true; we do not do that. Law enforcement only acts pursuant to a court order issued on a showing of probable cause that specific communications are being used in the furtherance of serious criminal activity.⁷ Only after a court order is issued can we intercept criminally related communication records if they are telephone communications, electronic communications, or e-mail traffic.⁸ With regard to encryption, what law enforcement seeks

tion, remote keyless entry systems, advanced messaging systems, and radio frequency communications systems").

6. See, e.g., Rob Dreher, *Is Big Brother Reading Your E-Mail?*, N.Y. POST, Oct. 21, 1999, at 6 (reporting on rumor that super-secret global surveillance network called "Echelon," headed by United States National Security Agency, monitors electronic transmissions and hones in on transmissions containing certain keywords (Unabomber, Anthrax, Fissionable Plutonium, North Korea, Militia, Delta Force, Ruby Ridge) which could signal national security threat).

7. See U.S. CONST. amend. IV. The federal statutes governing the use of wiretaps are found at 18 U.S.C. §§ 2510-2522 (1994), and include the following language:

(1) Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application. Each application shall include the following information: . . . (b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) . . . a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted.

18 U.S.C. § 2518(1) (1994).

8. See 18 U.S.C. § 2518. The federal wiretap laws were extended to include wireless voice communications and electronic communications such as e-mail or other computer-to-computer transmissions by the Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). See also Freeh Testimony, *supra* note 2, at 41-42 (em-

is a balanced encryption policy—one that puts strong, robust encryption in the hands of the general public for legitimate uses, while at the same time providing not a back door, but a Fourth Amendment front door, through which law enforcement can walk with a court order when encryption is used for criminal purposes.⁹

Generally, encryption affects law enforcement in two areas: electronic surveillance, and search and seizure. Electronic surveillance is used by federal law enforcement, and state and local law enforcement in one of the forty-four states that have enacted wiretap statutes,¹⁰ to intercept communications, pursuant to a court order, that are being used in the furtherance of serious criminal activity. Electronic surveillance is truly a technique of last resort.¹¹ A judge will only grant a wiretap court order after a showing that specific communications are being used in furtherance of serious criminal activity and that all other investigative techniques were tried and proved unsuccessful, or the alternate techniques are too dangerous to employ.¹² Some of the most important and significant information that has helped us prevent criminal activity and solve crimes has been obtained through the use of a court-ordered wiretap.¹³

The other area in which law enforcement is affected by encryption is search and seizure. Everyone is now using computers; paper files are disappearing. As a result, law enforcement must now seize more and more electronically stored, criminally related information being kept on hard drives, floppies, and other electronic storage devices. Therefore, law enforcement agencies need the ability to gain immediate access to the plaintext of those encrypted, criminally re-

phasizing that, with regard to search and seizure of encrypted materials, law enforcement is not seeking new constitutional powers, but “a fourth amendment that works in the information age”).

9. See Freeh Testimony, *supra* note 2, at 39.

10. See, e.g., N.Y. CRIM. PROC. LAW § 700.05-.70 (McKinney 1999).

11. See Freeh Testimony, *supra* note 2, at 42 (calling electronic surveillance “a very unique and very infrequently used technique” and noting that in 1996, only 1,149 electronic surveillance warrants were issued to federal, state, and local law enforcement).

12. See 18 U.S.C. § 2518(1)(c) (1994); *United States v. Giordano*, 416 U.S. 505, 515 (1974) (stating that in order to get wiretap, “the applicant must state and the court must find that normal investigative procedures have been tried and failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous”); *United States v. Thompson*, 944 F.2d 1331, 1339-40 (7th Cir. 1991) (holding wiretap properly authorized where it was unlikely that infiltration by informants would be successful).

13. See *Encryption, Key Recovery, and Privacy Protection in the Information Age: Hearing on S. 376 and S. 909 Before the Senate Comm. on the Judiciary*, 105th Cong. 44 (1997) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) (stressing that wiretapping is crucial in investigation of terrorism, espionage, organized crime, drug trafficking, public corruption, and violent crime).

lated communications or stored data files so we can carry out our public safety obligations, acting under the framework of the Fourth Amendment.

As Agent Rohmer pointed out, we are not seeing that much use of encryption. Approximately 9 percent of forensic computer files that are examined by the FBI have some type of encryption or password protection, and I think that is in line with the amount of encryption the general public is using—about 5 to 9 percent of the general public is using encryption. However, I think that is going to change.

Let me give you just a couple of case examples in which encryption was used. Agent Rohmer already pointed one out: Aldrich Ames used a commercially available encryption software package after he was instructed by a Soviet handler to start encrypting information to be sent to other Soviet handlers.¹⁴ Ramzi Yousef, an individual very familiar to the people of New York, used encryption in another case. Yousef was one of the masterminds of the World Trade Center bombing.¹⁵ When he was captured over in the Far East, one of the searches revealed that he had a laptop computer that contained information about a plot to blow up eleven U.S. commercial aircraft in that region.¹⁶ Some of the information on that computer was encrypted.

Law enforcement is also encountering encryption in many of our child pornography cases. One case, known as the “Innocent Images” case, involved a pedophile who was encrypting the pornographic images of children and e-mailing these images to a co-conspirator in another state.¹⁷

On another front, increasing numbers of drug traffickers along the southwest border of the United States are using encryption technology. As Agent Rohmer mentioned, the Drug Enforcement Administration (DEA) has now had over 500 individual intercepted telephone calls at the command and control level where drug cartels were using commercially available encryption products to encrypt their cellular phone conversations to prevent effective execution of the

14. See FEDERAL BUREAU OF INVESTIGATION, *supra* note 5, at 5.

15. See *id.* at 6; William M. Carley, *Explosive Theory: Bombing in New York Bears Some Hallmarks of Mideast Terrorists*, WALL ST. J., Mar. 1, 1993, at A1.

16. See FEDERAL BUREAU OF INVESTIGATION, *supra* note 5, at 6.

17. See *id.*; see, e.g., United States v. Lamb, 945 F. Supp. 441 (N.D.N.Y. 1996). “Innocent Images” is the name of an FBI initiative, which originated in 1995, in which FBI agents go on-line in an undercover capacity, posing as young children or sexual predators in order to identify individuals victimizing children. See *Preventing Child Exploitation on the Internet: Hearing Before the Senate Comm. on Appropriations*, 105th Cong. 12 (1998) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation). Since 1995, the “Innocent Images” investigation has generated 328 search warrants, 162 indictments, and 184 convictions. See *id.*

court-ordered intercept.¹⁸ Currently, these products do not have a means through which law enforcement, acting pursuant to a Fourth Amendment court order, can gain plaintext access to the encrypted communication.

Now, let me discuss law enforcement's ability to break encrypted information. The law enforcement community, unlike the intelligence community which is protected by export controls, is in the business of gathering evidence, not intelligence. Part of that process involves taking that evidence into a court of law. Under the Sixth Amendment, law enforcement must articulate how we obtained that evidence. As a result, law enforcement must divulge its capabilities to the defendant in open court—not specifically how we do it, but that we have a particular capability. Given this requirement, the capabilities of the intelligence community to decrypt encrypted information are not available to law enforcement, as it would undermine the intelligence community's mission if their capabilities had to be revealed.

Absent some form of key recovery or recoverable method,¹⁹ a brute force attack will not meet law enforcement needs. If we are working on a terrorist case and intercept a communication that we believe to be in furtherance of criminal activity, and that communication is encrypted—say with PGP, which is 128 bit encryption, a brute force attack to decode one PGP message, using a Cray computer, would take nine trillion times the age of the universe. If a communication involves a plot to shoot down a jumbo jet out of O'Hare Airport, and I intercept that communication but cannot obtain the plaintext to prevent the attack, I am going to find out about it only after that plane goes down. That is not a hypothetical—it actually occurred in Chicago. We prevented a jumbo jet from being shot down because we used a wiretap; fortunately, the terrorists were not using encryption. This is our greatest fear, that, one day, a terrorist attack will succeed because law enforcement could not gain immediate access to the plaintext of an encrypted message, lawfully seized prior to the attack being carried out. This is why the law enforcement community is advocating that commercially available encryption products have some technical means that allow a law enforcement agency, acting pursuant to a Fourth Amendment warrant, to gain immediate

18. For a discussion of DEA operations that intercepted encrypted cellular phone conversations between high-level cartel members, see Drug Enforcement Administration, *DEA Congressional Testimony*, U.S. DEP'T OF JUSTICE (Sept. 3, 1997) <<http://www.usdoj.gov/dea/pubs/cngrtest/ct970903.htm>>.

19. A key recovery or recoverable method would enable the immediate access to the plaintext of encrypted, criminally related data pursuant to a lawful court order. See FEDERAL BUREAU OF INVESTIGATION, *supra* note 5, at 7.

plaintext access to those lawfully intercepted, encrypted, criminally related communications or those lawfully seized, encrypted, criminally related computer files; that way, we can effectively carry out our public safety mission.

We are not advocating any one particular technical solution. You may have heard that law enforcement is advocating only a key recovery solution. This is not the case. Law enforcement believes that commercially available encryption products should have some means by which we can gain plaintext access pursuant to a court order. Key recovery is one option; key escrow is another option;²⁰ and recoverable products, such as those being built by Cisco Systems, is a third option.²¹ Cisco is a company that makes computer routers, which Cisco sells to Internet service providers. Cisco developed a “clear zone” within the router, whereby law enforcement can go to the systems administrator, provide a warrant, and receive the plaintext to those encrypted e-mail communications for which the warrant was issued.²² That is a solution that meets law enforcement’s needs perfectly.

The same holds true for personal communications systems, like Sprint Spectrum. The radio frequency link from the cellular phone to the tower is encrypted, but it is decrypted at the switch.²³ Obviously, when we conduct a wiretap, we use the cooperation of the telephone companies, and the telephone companies provide us with the plaintext of the cellular phone conversation. As you can see, there are products out there that are socially responsible, that meet law enforcement’s public safety needs while providing legitimate users with protection.

What truly concerns us are those end-to-end encryption products, either hardware or software, that can be attached to any phone in the United States, or the world for that matter. As long as your co-conspirator has a similar device, you can talk encrypted from end to end and law enforcement cannot gain plaintext access, even though the

20. See generally NATIONAL RESEARCH COUNCIL, *CRYPTOGRAPHY’S ROLE IN SECURING THE INFORMATION SOCIETY* 359 (Kenneth W. Dam & Herbert S. Lin eds., 1996) (defining “key escrow” as “an encryption system that enables exceptional access to encrypted data through special data recovery keys held by a trusted third party”).

21. See *Internet Commerce, Encryption*, CISCO SYSTEMS (last modified Nov. 18, 1998) <<http://www.cisco.com/warp/public/779/govtaff/policy/e-commerce/issues/encryption.shtml>>.

22. See *id.* (“Cisco advocates a non-cryptographic alternative to key-recovery called ‘Clear Zone.’ It is a dynamically created and managed access point that allows the operator of an encrypting device to comply with a legal warrant without giving away a key or weakening overall security.”).

23. See NATIONAL RESEARCH COUNCIL, *supra* note 20, at 327 n.9.

conversation relates to serious criminal activity. We can intercept those communications, but cannot decrypt or translate them because those encryption products, generally speaking, are currently made in a non-recoverable format. It is the same way with software products. Most of the software encryption products do not possess some type of recovery feature. It is technically possible to include a recovery feature as part of the software; but, right now, it is not being done.

In closing, the Clinton Administration has chosen to adopt a position on encryption that is supportive of both the public safety needs of law enforcement as well as the national security needs of the intelligence community. To achieve these goals, the Administration will maintain export controls on encryption products to ensure that national security needs are met, and will continue to request, on a voluntary basis, that companies who manufacture encryption products for use in the United States manufacture recoverable encryption products that allow law enforcement access to plaintext, pursuant to a court order.²⁴ Discussions with industry regarding law enforcement's public safety needs have been ongoing since April of 1993. The recent relaxation of encryption export controls for certain business sectors and for recoverable encryption products are a reflection of that policy.²⁵ The Administration has been attempting to use export controls to influence the development and use of recoverable encryption products within the United States. Currently, there are absolutely no restrictions on domestic encryption products, whether the product is manufactured in the United States for domestic use or is imported into the United States. In the past, there was never a need for domestic controls on encryption products because, unlike today, these products were not generally available for use by the public at large, including criminals and terrorists; thus, in the past it was not an issue that impacted public safety.

24. See FEDERAL BUREAU OF INVESTIGATION, *supra* note 5, at 8.

25. The Clinton Administration released revised encryption regulations on December 31, 1998. See Christina A. Cockburn, Comment, *Where the United States Goes the World Will Follow—Won't It?*, 21 Hous. J. INT'L L. 492, 507 (1999). Cockburn lists the following changes made by the new regulations: (1) allowing 56 bit encryption products without key recovery after a onetime review; (2) loosening the requirements for encryption products stronger than 56 bits that contain key recovery; (3) permitting exports of "recoverable products" to foreign commercial firms for internal company proprietary use in select countries; and (4) loosening restrictions by allowing certain U.S. subsidiaries, insurance companies, companies in the health and medical sector, and on-line merchants to use unlimited encryption. See *id.* at 507-09. See, e.g., Encryption Items, 63 Fed. Reg. 72,156 (1998) (to be codified at 15 C.F.R. pts. 740, 742, 743, 772, 774).

Based on the Administration's current encryption policy, the only restrictions on encryption products will continue to be export controls to address national security interests and the mission of the intelligence community. The Administration will continue to try to address law enforcement's public safety needs concerning encryption products for domestic use through voluntary efforts.

Our distinguished panelist indicated earlier that the Administration's policy fails to explain how law enforcement would go about obtaining recoverable information.²⁶ Well, let me answer that. We would obtain the criminally related information through a court order used to either seize communications or seize computer files, pursuant to the Fourth Amendment. If policy makers in Congress choose to require a secondary court order should someone escrow key recovery information, the law enforcement community would be more than willing to get a secondary court order to obtain plaintext access to the recovery information after we have already obtained the encrypted, criminally related communication or electronically stored information. We are happy to do that, and have already unanimously indicated our approval to Congress.

Lastly, encryption-related legislation was recently introduced in Congress by several different camps.²⁷ Industry leaders convinced several members of Congress to introduce legislation to relax all existing export controls on encryption products, regardless of the impact on public safety and national security. Law enforcement and, more importantly, national security entities have rejected that, as did the Administration, because of its obvious consequences. We, in the law enforcement community, support legislation that is balanced and responsible, and that meets legitimate users' needs for strong encryption, while at the same time meeting our public safety obligation to protect and lawfully seize criminally related information and gain plaintext access. In the end, no encryption-related bills were passed during this last Congress.

26. See Marc S. Friedman, *Some Observations on Encryption—Plain, Simple, and Unencrypted*, 3 N.Y.U. J. LEGIS. & PUB. POL'Y 5, 9-10 (1999).

27. See FEDERAL BUREAU OF INVESTIGATION, *supra* note 5, at 8-10. See, e.g., Security And Freedom through Encryption (SAFE) Act, H.R. 850, 106th Cong. (1999); Encryption Protects the Rights of Individuals from Violation and Abuse in Cyberspace (E-PRIVACY) Act, S. 2067, 105th Cong. (1998); Security and Freedom Through Encryption (SAFE) Act, H.R. 695, 105th Cong. (1997); Computer Security Enhancement Act of 1997, H.R. 1903, 105th Cong. (1997); Communications Privacy and Consumer Empowerment Act, H.R. 1964, 105th Cong. (1997); Encryption Communications Privacy Act of 1997, S. 376, 105th Cong. (1997); Promotion of Commerce On-Line in the Digital Era (PRO-CODE) Act of 1997, S. 377, 105th Cong. (1997); Secure Public Networks Act, S. 909, 105th Cong. (1997).

The Intelligence Committee in the House did introduce a bill that we believed was balanced.²⁸ The bill somewhat relaxed export controls, but established domestic controls that were reasonable from law enforcement's perspective. Under the bill, all commercially available encryption products for confidentiality would be required to have some technical means by which we could gain plaintext access to encrypted, criminally related information, pursuant to a court order.

So, the debate is still raging and we, in the law enforcement community, continue to meet with members of the industry—Bill Gates, Jim Barksdale from Netscape, and others.²⁹ These industry leaders recently agreed that we have legitimate needs; the objective here is to try to find some way that allows us to continue to do our job effectively and protect public safety while at the same time not disadvantaging U.S. industry.

28. *Cf.* Freeh Testimony, *supra* note 2, at 42-43 (“Except for 909, the other pieces of legislation do not, in my view, attempt to balance those two interests at all.”).

29. *Cf. id.* at 39-40 (noting extraordinary risk in trusting public safety needs to market forces).