

SOME OBSERVATIONS ON ENCRYPTION—PLAIN, SIMPLE, AND UNENCRYPTED

*Marc S. Friedman**

I want to thank you very much for having me here today. Before I actually start, I just want to make some observations that are very personal to me, and I want to tell you a little story that, in a sense, will allow you to understand my orientation and approach to this topic.

First, the irony: During the prior presentation, I made a note to myself that the word “distinguished” was used five times by two speakers in connection with this panel that includes me. For me, it is a nice irony to know that I am being welcomed as a distinguished authority at a law school where my application for admission was rejected.

Second, whenever I appear at law schools to speak on one topic or another, my mind naturally wanders back to when I was in law school. I attended law school between the years of 1968 and 1971, years of tremendous turbulence here in the United States. I had the very good fortune, from my point of view, of attending law school five blocks west of the White House. And, when I was in close proximity to FBI agents as a law student, I would usually look to see whether they were trying to take pictures of me as I participated in different demonstrations. I do want to say today, though, that it is really a delight to be sharing this platform with two very distinguished representatives of the government, and I am really looking forward to hearing what they have to say.

Third, how did I get involved with encryption? There was some reference made to a case that I had won; it was actually in 1979. In 1978, just after I opened my law firm, Friedman Siegelbaum, a fellow named Ed Chatlos walked into my office. He said that he had purchased a computer from National Cash Register Association, as it was then named, and the thing did not work. Well, when I was in

* Marc S. Friedman is a founding partner of the law firm of Friedman Siegelbaum LLP, and is the President-elect of the Computer Law Association. He is an Adjunct Professor of Law, Seton Hall University Law School, and a co-author of *A Vendor's Guide to Computer Contracting*.

college and in law school, we did not have computers. I did not have my first pocket calculator until I was already practicing law for two years. So, I knew nothing about the product and I knew nothing about the technology. Nonetheless, I took on the case and filed a lawsuit, *Chatlos Systems v. National Cash Register Corp.*,¹ in which we sought compensatory damages of \$440,000 as a result of a computer system that had failed.

After a four week trial in federal court in Newark, we got a judgment in which we were awarded only \$140,000.² Frankly, this was a very lukewarm result considering what we were asking for. So, I was sitting in my office, reading this opinion and saying to myself, "Well, I am not terribly excited about it, but there may be other people who are." I then called a friend of mine at the *Star-Ledger*, a regional newspaper, and said, "Look, I just won this case. Maybe you would be interested in it. Go down to the courthouse, take a look at the file, and if you have any questions, call me back." One day goes by; two days go by; and on the third day, there was a very nice little story in the *Star-Ledger*. I was a young lawyer and my head swelled. The story was picked up by the Associated Press and the next day, that story was in every single newspaper in the United States and Canada. Within hours, I was regarded as the world's leading expert in this new emerging area of computer technology law.

I tell you that story for two reasons. First, for those of you who are law students, to let you know that, at least for some of you, someday someone is going to walk into your office and send your career off in a different direction from anything you could have ever expected. Second, I tell you that story to show that my involvement in these matters has largely been as a private practitioner representing business clients. In essence, I bring to today's program two points of view: first, as a child of the 1960s who passionately believes that the rights of privacy and free expression are the bedrock of what makes this country great, and second, as an attorney with clients involved in electronic commerce, who want to have the maximum opportunity to sell their goods and services in this country, as well as overseas. That brings me to my remarks.

My duty as the first speaker is not just to express a point of view, but also to help frame the issue. As you can see, there are certain legitimate government concerns regarding the use of encryption. We know that there is an increasing use of computer communications by

1. 479 F. Supp. 738 (D.N.J. 1979).

2. *See id.* at 749.

organized crime, by isolated and disorganized groups of criminals, by terrorists, and by those engaged in espionage. My colleagues here could probably speak for days about these subjects. We all know that computer communication may be the principal way in which conspiracies are facilitated. So, what we have is a situation where there is a real need to intercept these computer communications made in the furtherance of crime, terrorism, and espionage. I do not think there is anyone in the room who could take the position that even those kinds of communications should be protected from surveillance.

The encryption issue is really, in a sense, the natural development of the government's eagerness to continue and increase its wiretapping activities. In preparation for today, I happened to look at some wiretapping statistics and, without getting into the details, I see that the number of wiretaps increases every year.³ And yet, statistically, the number of incriminating conversations that are surveilled tends to go down.⁴ The percentage tends to go down as the numbers of conversations that are being surveilled goes up.⁵ This strongly suggests to me that there is at least a possibility that wiretap abuses are taking place. I am not here to inculcate anyone; however, that statistic raises my eyebrows.

The encryption issue is really an attempt to further increase the government's wiretapping and surveillance capabilities by restricting the efficacy of encryption devices and by introducing a key escrow system. In June of 1996, this point was made very clear by Attorney General Janet Reno, who stated that "[e]ncryption, as a practical matter, diminishes the power of law enforcement to do its job The consequences of our losing the ability to wiretap would be enormous."⁶

What we now see in the encryption area is an attempt to expand the federal government's power. We know from policy statements, regulations, and other utterances that the Clinton Administration has sought to increase the power to surveil computer communications by controlling the technology that prevents surveillance. It is this policy

3. See Jim McGee, *Wiretapping Rises Sharply Under Clinton*, WASH. POST, July 7, 1996, at A1; Laurie Asseo, *State-Approved Wiretaps Rose 24% Last Year*, US Reports, BOSTON GLOBE, May 6, 1999, at A16.

4. See Barry Steinhardt, *Wiretaps: Danger To Liberty Or Vital Tool?: New Legislation Authorizes Wholesale Invasion Of Privacy*, ST. LOUIS POST-DISPATCH, Nov. 5, 1996, at 11B.

5. See *id.*

6. Attorney General Janet Reno, *Law Enforcement in Cyberspace*, Address By The Honorable Janet Reno Before the Commonwealth Club of California (June 14, 1996), available in <<http://zeus.bna.com/e-law/docs/reno.html>>.

which really gives rise to the issues that we are going to talk about today and to the different points of view that you are going to hear.

In September, there were some fairly substantial changes made to the Administration's policy concerning encryption and the control of encryption devices.⁷ I think these changes are progressive, useful, necessary, and admirable. The issue, though, is whether the changes that have been made to the policy are significant enough to address the privacy concerns and commercial concerns of the business community.

Now, before I get into the policy changes, let me get technical for just a moment, although my guess is that my colleagues could probably give a better explanation of this. A "bit," as probably many of you know, is the unit by which the encryption key length or strength is measured. The more bits in the encryption, the stronger the encryption. Just by way of example, if you use an encryption that has a key length of 40 bits, when you do the mathematics, there are a billion possible keys that can use encryption of 40 bit length. If it is a 56 bit length encryption, there are 72 trillion possible schemes. If you use a 128 bit encryption, it is a gazillion—I do not know how many sets of zeros before you get to a number. There are a gazillion different keys that can be used when you are using 128 bit encryption devices. What that means, in essence, is that, if I were a smart computer guy, I might be able to sit down with a 40 bit device and figure it out with minimal resources. I might even be able, if I had the time and resources, to figure out a 56 bit encryption. But, if I am faced with 128 bit encryption, I am never going to be able to crack that device. That is what we are talking about when we say weak encryption and strong encryption.

The first new policy change decontrols encryption devices of up to 56 bits.⁸ In other words, it will permit the export of up to 56 bit encryption devices which, nonetheless, will be subject to a onetime government review. This is a relaxation of the policy that preexisted this change, where these devices could not be exported so freely.

This policy change also provides export relief for specific industry segments.⁹ It will permit the export of products stronger than 56 bits to overseas subsidiaries of U.S. corporations, the health and insurance industries, and undefined and unspecified electronic commerce users. These devices will still be subject to a onetime government

7. See Joel Brinkley, *U.S. Eases Encryption Software Export Bans*, N.Y. TIMES, Sept. 17, 1998, at C5.

8. See generally Christina A. Cockburn, Comment, *Where the United States Goes the World Will Follow—Won't It?*, 21 Hous. J. INT'L. L. 492, 507-09 (1999).

9. See generally *id.*

review and you will need an export license to take advantage of the new policy, but it is an advancement.

Next, the new policy provides exemptions for recoverable products.¹⁰ The new policy, when implemented, will permit the export of encryption products of, not just 56 bits, but up to 128 bits, if: (1) the product includes back door access, which is a way to get through the encryption device to see the plaintext; (2) the product uses a key recovery system, which means that an entity that has a key can unlock the device; or (3) the product permits access to the text of the communication through a system administrator, or some other person independent of the user.

Now, those exemptions are all advancements. Even organizations that are concerned about the privacy aspects of this issue applaud this change in administration policy. However, these changes do not fully alleviate the business community's concerns.

Problem number one: The 56 bit encryption is not going to adequately protect on-line privacy and security, according to many experts.¹¹ Just last summer, a group in California developed a device called the DES Cracker that broke a 56 bit encrypted message in just, coincidentally, 56 hours, using very limited resources.¹²

Problem number two: Granting export relief for industry groups leaves out individuals such as human rights workers—folks I happen to sympathize with—and other non-commercial groups who have a very strong interest in protecting the privacy of their electronic communications. Furthermore, these individuals will not be able to take advantage of the new export regulations unless they use products with back doors that will allow law enforcement and others to decode their messages and see the text. The Administration seems to want to continue its policy to use export controls, although relaxed, to force the adoption of key recovery systems that would allow outsiders to penetrate the encryption device and view the underlying message or information.

Problem number three: The new policy statement is totally bereft of any standards that would say when the government can or should

10. *See generally id.*

11. *See "EFF DES Cracker" Machine Brings Honesty to Crypto Debate, Electronic Frontier Foundation Proves that DES is not Secure*, ELECTRONIC FRONTIER FOUNDATION (July 17, 1998) <http://www.eff.org/pub/Privacy/Crypto_misc/DESCracker/HTML/19980716_eff_descracker_pressrel.html> (stating that it took machine less than three days to crack encoded messages).

12. *See id.*

be able to access the so-called plaintext or underlying part of the encrypted message.

By examining the Administration's new proposal in this framework, seeing the good, the bad, and the ugly, it helps us focus on what I think is the core issue: Will the new encryption policy, as embodied in legislation and regulation, adequately protect the privacy rights of citizens and ensure that U.S. companies can compete fairly in the world marketplace, while also giving law enforcement the tools necessary to detect, prevent, and prosecute crime, terrorism, and espionage?

Now, obviously, there are different points of view. You saw the Administration's point of view. You will hear the FBI's and the Secret Service's points of view shortly, although I am certain we can reasonably anticipate what each of these other distinguished speakers are going to say.

As an American Civil Liberties Union Special Report recently concluded, "We are now at a historic crossroads: we can use emerging technologies to protect our personal privacy, or we can succumb to scare tactics and to exaggerated claims about the law enforcement value of electronic surveillance and give up our cherished [constitutional] rights, perhaps – forever."¹³ That is the issue. Those are the points of view, broadly drawn.

13. See *Big Brother in the Wires, Wiretapping in the Digital Age*, AMERICAN CIVIL LIBERTIES UNION (Mar. 1998) <http://www.aclu.org/issues/cyber/wiretap_brother.html>.