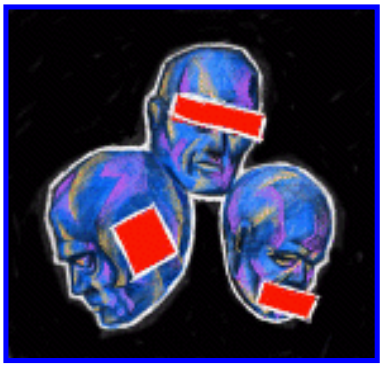
Digital Liberties

Free Speech And Privacy Under Attack In Cyberspace

Lorrie Faith Cranor



> *Cyberspace is the ``place'' where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city.* The place between *the phones. The indefinite place* out there,*where the two of you, human beings, actually meet and communicate.*
>
> --Bruce Sterling [***The Hacker Crackdown***]

Citizens of cyberspace who find their physical feet resting firmly on American soil are not immune to the long arm of U.S. law. And as the number of Americans journeying into cyberspace increases, some Congressional representatives and government agencies are rushing to extend U.S. laws even further into the virtual world. While supporters applaud efforts to create laws for cyberspace that provide the same protections that U.S. citizens have come to expect in the physical world, opponents say the virtual world equivalents have much broader implications than their physical world counterparts.

The Digital Telephony Bill, the Clipper chip, and recently the Communications Decency Act have all sparked controversy about the right to free speech and communications privacy in cyberspace. In this virtual world, where existence itself is defined by the ability to communicate, it comes as no surprise that this has become the center of controversy.

Digital Telephony

Worried that the propagation of digital communications technology would prevent law enforcement officers from conducting court authorized wiretaps, the Federal Bureau of Investigation (FBI) **proposed legislation** in March 1992 to make it easier for law enforcement officers to monitor U.S. communications systems. The FBI proposal included provisions requiring all communications systems to be designed to facilitate law enforcement monitoring from a remote location. If passed, the legislation would have applied to a wide range of communications systems and providers including public electronic mail systems, telephone systems, computer bulletin boards, online information services, Internet service providers, cellular communications systems, and others.

The FBI's concerns were based on the surveillance challenges posed by new telephone systems, which use digital technology rather than the traditional analog technology. In a digital system, sound waves are converted into strings of 1s and 0s which are transmitted as digital signals to a receiver that converts them back to sound

waves. Intercepting the digital signal is useless unless you can convert it back to its original form. Sophisticated equipment is required to identify and intercept a particular conversation in the stream of digitized conversations traveling across digital communications systems.

Ever since the passage of the 1968 Omnibus Crime Control and Safe Streets Act, communications service providers have been required to assist law enforcement officers in conducting court ordered wiretaps. Historically, there have been few technical problems encountered while attempting to carry out court ordered wiretaps. To tap a traditional analog telephone system, all one must do is intercept and amplify the electronic signals that travel through the phone lines. The interception can be done with a simple metal clip connected by a wire to a small tape recorder.

FBI statements said the proposed legislation was designed to ensure that law enforcement officers continue to have the same wire tap ability that they enjoyed with analog phone systems. However, opponents of the proposal said it would go beyond simply extending the status quo.

The FBI's proposal was opposed by a large number of computer and communications companies and industry associations, as well as the American Civil Liberties Union, **Computer Professionals for Social Responsibility**, and the **Electronic Frontier Foundation** (EFF). A **white paper** prepared by the EFF in coalition with 35 other organizations and companies criticized the proposal for being vague, expensive, overly broad, and possibly unnecessary. EFF was particularly critical of the requirement that wiretap facilities be built into all communications systems: ``The current wiretap statutes take the communications networks as they find them and do not require any provider of communications service to redesign the system, or to refrain from using any particular technology, solely on the ground that such a technology would make interception more difficult."

The proposed legislation was met with so much opposition that it never received a sponsor in the 102nd Congress. However, on December 8, 1993 FBI Director Louis Freeh announced that the proposal would be reintroduced. In a **speech at the National Press Club** he explained, ``Telephone's digital technology has advanced in such a way that criminals will be able to avoid law enforcement detection simply by using the telephone. They will be able to conduct their illicit businesses openly and without any fear of the consequences. In order to keep up with the criminals and to protect our national security, the solution is clear: we need legislation to ensure that telephone companies and other carriers provide law enforcement with access to this new technology."

In March 1994, the FBI released a new draft of the proposed wiretap legislation, which received Clinton Administration support. EFF responded quickly, stating, ``In short, the bill lays the groundwork for turning the National Information Infrastructure into a nation-wide surveillance system, to be used by law enforcement with few technical or legal safeguards."

Despite continued opposition, the political climate in Washington was such that EFF leaders were not optimistic that they could prevent the proposed legislation from passing. Therefore, EFF worked with Senator Patrick Leahy (D-VT) and Representative Don Edwards (D-CA) to draft a narrower bill that would meet the needs of law enforcement without sacrificing communications privacy. The **Edwards/Leahy Digital Telephony Legislation (HR 4922/S 2375)** excluded providers of online services from the wiretap

requirements and included privacy protections absent from the FBI's proposals.

But many of the organizations that had opposed the FBI proposals, continued to oppose the new compromise legislation. The Electronic Privacy Information Center (EPIC), the **Voters Telecomm Watch**, the American Civil Liberties Union, and many other organizations supported a grassroots campaign to oppose the measure. As thousands of online activists contacted their senators and representatives, several congressional offices reported that their fax machines were swamped with letters opposing the wiretap legislation during the final weeks that Congress was in session. ``The grassroots campaign that emerged to oppose the wiretap legislation shows the potential of the Internet as a means of educating the public and promoting democratic participation in the policymaking process," boasted an **EPIC statement**.

However successful the grassroots campaign proved to be in educating the public, it ultimately failed to prevent passage of the Edwards/Leahy legislation. On October 7, just when Internet activists began breathing sighs of relief that the bill would not pass before the end of the 103rd Congressional session, the Senate approved the measure by unanimous consent without any floor debate.

Some Net activists remain critical of the EFF for not opposing the legislation, while others applaud them for helping achieve a compromise. In a **public statement** Jerry Berman, then EFF's Policy Director, said, ``Although we remain unconvinced that this legislation is necessary, the bill draws a hard line around the Internet and other online networks." He added, ``The fact that the Internet, BBS's, Prodigy, and other online networks are not required to meet the surveillance capability requirements is a significant victory for all users of this important communications medium."

The Clipper Chip

Despite the grassroots campaign against digital telephony, the legislation did not get nearly as much attention as the Clipper Chip -- perhaps the most well known icon of the communications privacy conflict. Introduced by the Clinton administration in April 1993 as part of the Escrowed Encryption Initiative, the Clipper Chip is designed to provide Americans with private communications channels that cannot be abused by criminals and terrorists. Telephones equipped with Clipper Chips can transmit and receive encrypted messages that are indecipherable to most eavesdroppers. However, an eavesdropper who obtains a special decryption key can decipher the messages.

Each Clipper Chip is assigned a unique serial number and decryption key at the time of manufacture. The decryption key is a very large number that can be plugged into a series of mathematical operations to decode an encrypted message. Each decryption key is split into two parts and stored or ``escrowed" by the **U.S. Treasury Department** and the **National Institute of Standards and Technology (NIST)**. These escrowed key halves are available only to law enforcement officers who obtain court authorization to conduct wire taps. An encrypted message cannot be decrypted without both parts of the decryption key.

Concerned that the unrestricted use of cryptography will make it difficult for law enforcement officers to catch criminals, the National Security Agency (NSA) developed the Clipper Chip, the underlying classified cryptographic algorithm SKIPJACK, and a data encryption chip called Capstone. In February 1994, this collection of encryption tools was approved by NIST as part of the Escrowed Encryption Standard (EES). As a

voluntary Federal standard, EES may be adopted by any government agency, which in turn could require that it be used for all electronic communications with that agency. However, there is no requirement that EES be used for any non-governmental communications.

Nonetheless, when EES was introduced, law enforcement agencies hoped that consumers purchasing secure telephones would voluntarily select Clipper products because of the Clipper Chip's high level of security and relatively low cost. They predicted that Clipper would become the de facto public encryption standard, used by anyone who values privacy -- including criminals. This would prevent the standardization of an encryption system that law enforcement agents could not break. ``What worries law enforcement agencies...is a world where encryption is standardized and ubiquitous.... In such a world, every criminal will gain a guaranteed refuge from the police without lifting a finger," explained Stewart Baker, former general counsel for the NSA, in a ***Wired*** article last year. ``In short, as long as legitimate businesses use key escrow, we can stave off a future in which acts of terror and organized crime are planned with impunity on the public telecommunications system."

But even before it was approved, EES was met with strong opposition from privacy advocates, the computer and telecommunications industries, and the online community. Opponents complained about a number of problems with EES including the potential for abuse by unscrupulous officials, the fact that the classified SKIPJACK algorithm is not available for public scrutiny, and difficulties likely to be encountered in marketing Clipper products outside the United States.

Clipper proponents tried to dismiss concerns about potential abuse, citing requirements for court authorization and extensive auditing. ``Even if you're worried about illegal government taps, key escrow reinforces the existing requirement that every wiretap and every decryption must be lawfully authorized. The key escrow system means that proof of authority to tap must be certified and audited, so that illegal wiretapping by a rogue prosecutor or police officer is, as a practical matter, impossible," explained Baker. But opponents remained unconvinced.

A February 1994 Time/CNN pole of 1,000 Americans found that two-thirds of those polled valued private phone calls more than the ability of police to conduct wiretaps. ``When informed about the Clipper Chip, 80% said they opposed it," *TIME* reported.

In addition, opponents were skeptical that EES would prove useful for law enforcement. At a **May 3, 1994 hearing** of the Senate Judiciary Subcommittee on Technology and the Law, Senator Leahy stated, ``I have serious questions about whether any sophisticated criminal or terrorist organization is going to use the one code endorsed by the U.S. Government and for which U.S. Government agents hold the decoding keys. There are a multitude of alternative encryption methods commercially available. If Clipper Chip does become the standard encryption method used by Americans, criminals may be forced to use Clipper to communicate with legitimate outsiders. But this is a big `if.'"

Even former acting NIST director Ray Kammer, an EES supporter who was involved in the development of EES, said, ``It's obvious that anyone who uses Clipper for the conduct of organized crime is dumb."

Opponents have speculated that EES would only be useful to law enforcement if all other forms of encryption

were outlawed. ``It is increasingly hard for me to imagine any other purpose for the Clipper/Skipjack operetta if not to prepare the way for the restriction of all private cryptographic uses to a key escrow system," wrote **EFF** Cofounder **John Perry Barlow** in the November 1993 *Communications of the* ***ACM***. But there have been no serious proposals to outlaw non-escrowed encryption in the United States. However, some Clipper opponents fear that a future administration, perhaps faced with a pending emergency, might try to convert a key-escrow standard into a key-escrow requirement. They view EES as the first step towards such a future plan.

Opponents are also suspicious of Clipper because the SKIPJACK algorithm has not been released for public scrutiny. Cryptographic algorithms are usually published and subsequently analyzed for weaknesses by cryptographers from around the world. One of the characteristics of strong encryption algorithms is that messages encrypted with these algorithms cannot be decoded without the proper decryption key. An eavesdropper who does not have the decryption key cannot decode the message, even if he or she knows the encryption algorithm used. The only way for an eavesdropper to decode the message is to guess the secret decryption key.

Some people are also suspicious that the SKIPJACK algorithm might include a secret weakness that would allow law enforcement officers to intercept and decrypt messages without obtaining court authorization. Such a weakness is often compared to the key holes in combination locks sometimes found on school lockers. While each student must use a secret combination to open his or her locker, the teachers can open all the lockers in the school with a special key. EES opponents say they cannot be certain that SKIPJACK does not include a weakness like this unless they are able to examine the classified algorithm.

But EES proponents maintain that the SKIPJACK algorithm must remain classified to prevent people from bypassing the mechanism that allows law enforcement officers to decrypt messages using the escrowed keys. At the May 3, 1994 hearing, Georgetown University Computer Science Professor **Dorothy Denning** **testified** that publication of the SKIPJACK algorithm ``would enable someone to build a hardware or software product that used SKIPJACK without escrowing keys, thereby taking advantage of the government's strong algorithm in order to make communications immune from lawful interception and foreign intelligence operations." But less than a month later Matt Blaze, an AT&T Bell Laboratories researcher, figured out how to do just that, despite the fact that the SKIPJACK algorithm remained classified.

On June 2, 1994 EES took a major blow when the *New York Times* reported that Blaze had discovered a way to **alter the Capstone chip output** so as to make the escrowed encryption keys useless. The NSA did not dispute this flaw, but maintained that the flaw would be too difficult and time consuming for anyone to exploit. Nonetheless, Clipper opponents began predicting the end of the Administration's support for EES.

The end finally came on July 20 when **Vice President Al Gore wrote to then Representative Maria Cantwell** to announce that the Administration planned to work with industry representatives and privacy advocates to develop a new ``key escrow encryption system that will provide strong encryption, be acceptable to computer users worldwide, and address our national needs as well." Gore wrote, ``The Administration understands the concerns that industry has regarding the Clipper Chip. We welcome the opportunity to work with industry to design a more versatile, less expensive system. Such a key escrow system would be implementable in software, firmware, hardware, or any combination thereof, would not rely upon a classified

algorithm, would be voluntary, and would be exportable."

While many EES opponents hailed Gore's letter as a victory, they were quick to point out that their battle was far from over. Gore made no promises to abandon the Clipper Chip, nor did he provide much information about the new key escrow system that would be developed. The letter merely marked the end of the current EES as the Administration's primary solution to law enforcement's encryption problem.

Communications Decency Act

Ever since Gore announced that the administration would rethink the EES, and the much protested digital telephony act was easily approved minutes before the end of the 1994 Congressional session, the communications privacy debate has proceeded without its former sense of urgency. The Net community is still in disagreement over whether the telephony bill compromise negotiated by EFF was a victory. And most people aren't willing to believe that the key escrow initiative is gone for good. But there's no longer a tangible chip or bill to rally around, and thus the uproar over privacy rights has died down.

But Net activists aren't resting. On February 1, just when it looked like things would be calm for a while, Senator Jim Exon (D-NE) introduced the ``**Communications Decency Act of 1995**" (S 314). Designed to ``extend and strengthen the protections which exist against harassing, obscene and indecent phone calls to cover all such uses of all telecommunications devices," the bill could have far reaching implications for freedom of speech on electronic networks.

``I want to keep the information superhighway from resembling a red light district," said Exon as he introduced the bill, which is identical to an **amendment** that he offered last year to the Senate Telecommunications reform bill. ``This legislation will help stop those who electronically cruise the digital universe to engage children in inappropriate communications and introductions or electronically stalk users of computer networks."

But opponents say that Exon's legislation goes beyond extending and strengthening existing measures. ``The Exon bill would not ... simply apply existing law to new telecommunications devices. Because of differences between existing telephone technology and telecommunications technology such as electronic messaging, the Exon bill would potentially prohibit a wide array of currently allowed electronic communications," wrote **James T. Bruce and Richard T. Pfohl on behalf of the Electronic Messaging Association** (EMA).

In addition, opponents say that besides punishing those who misuse communications networks by sending indecent, lewd, threatening, or harassing messages, the bill would place criminal liability on the owners and operators of networks that do not prevent such misuse. In order to avoid such liability, network operators would have to pre-screen every transmission over their networks -- a task that would likely be both illegal and impossible. ``This bill raises fundamental questions about the ability of government to control content on communications networks, as well as the locus of liability for content carried in these new communications media.... S. 314 would expand current law restricting indecency and harassment on telephone services to all telecommunications providers and expand criminal liability to *all* content carried by *all* forms of telecommunications networks," explained the **Center for Democracy and Technology (CDT)** in an **analysis of the legislation**.

However, during a **February 13 CNN panel discussion** with EPIC director Marc Rotenberg, Exon denied that he had intended the bill to have such broad implications. ``That's like saying we're going to put the mailman who delivers the smut in jail. That is not our intent at all," Exon said.

On March 23 the Senate Commerce Committee approved a modified version of the Exon bill as an amendment to the Telecommunications Competition and Deregulation Act of 1995. Although this version removes some of the liability potential for online service providers, opponents still say the bill would be a violation of civil liberties.

Opponents remain critical of the bill for treating the online interactive media as mass media. ``As Congress moves to regulate new interactive media, it is essential that it understand that interactive media is different than mass media. The power and flexibility of interactive media offers a unique opportunity to enable parents to control what content their kids have access to, and leave the flow of information free for those adults who want it. Government control regulation is simply not needed to achieve the desired purpose," stated CDT.

In addition, opponents say that applying laws intended for telephones or mass media to computer bulletin boards and the Internet is not always appropriate. EMA points out that the courts have interpreted the obscenity prohibitions in the Communications Act of 1934 to apply only to non-consensual or unsolicited telephone calls. Applying this rule to online media is difficult. ``Electronic bulletin boards and discussion groups blur the concept of intent: anyone has the potential to stumble, as if accidently stumbling into an X-rated movie theater, upon indecent material. Such an encounter may not be `consensual,'" EMA explained. ``Numerous electronic bulletin boards on line contain indecent material, and indecent material may spring up in any discussion group, or even when a rap artist discusses his lyrics, or a record company puts a new release on line."

But Exon has made statements suggesting that it is just this sort of material that he intends to eliminate. ``Right now there is a bulletin board that almost anyone can check into," said Exon, in apparent reference to Usenet -- a publicly accessible Internet distributed bulletin-board-like-system with thousands of discussion areas called newsgroups. ``It lists different subjects. It goes into sex. You can plug into that, and you can get all kind of lewd, obscene smut material. I think we've got to take some action now before this gets out of hand."

The Debate Continues

The future of the Exon bill, escrowed encryption, and even freedom and privacy in cyberspace remains uncertain. The issues being debated are much more fundamental than whether or not to pass a bill or propagate an encryption chip.

There are questions about the very nature of cyberspace. Should it be governed as a place, a broadcast medium, a publication, or as a unique thing for which new legal precedent must be established? Should it be governed at all?

There are also questions about rights and responsibilities. Is the government's responsibility to maintain national security and prevent crime more important than the individual's right to privacy and free speech? Is it

possible for government to do its job without sacrificing individual rights, or must individuals pay a price in order to enjoy safety for themselves and their children?

Cypherpunk Tim May described the encryption and privacy controversy as a debate between those who feel that their communication is ``none of your damn business'' versus those who ask, ``What have you got to hide?''. Washington University Computer Science Professor Doug Schmidt described it as a debate between those who consider government to be a ``guardian of civilization'' versus those who consider government to be a ``usurper of individual liberties.''

When cyberspace was truly a new frontier, inhabited only by the pioneering elite, questions about rights, responsibilities, and sovereignty seemed inconsequential. But as more and more people storm the Internet, cyberspace is becoming an extension of our society.