19. Freedom on the Internet and Other Computer Networks

Congress should

- repeal the Communications Decency Act and reject "harmful to minors" substitutes;
- lift restrictions on the export of strong cryptography;
- reject mandatory key recovery;
- reject hasty amendments to the copyright law, such as those suggested in the Clinton administration's "White Paper on Intellectual Property"; and
- reject attempts to restrict anonymous computer communications.

In responding to the many voices that speak through the Internet and other computer networks, the United States can set the entire world an example of commitment to freedom of speech and privacy rights. From Argentina to Zambia, governments have recognized information provided over the Internet as a powerful threat to their oppressive regimes. Singapore and China, among others, have moved aggressively to censor newsgroups and Web sites.

It would be shameful for the United States to follow such examples. This Congress has the opportunity to reverse a number of unfortunate policies that make it appear that the United States is not, in spite of our heritage, a champion of liberty online.

Computer Networks—Past, Present and Future

The Internet sprang up from a rudimentary Department of Defense network known as the ARPANET (ARPA stands for the Advanced Research Projects Agency). By the 1980s hundreds of universities, corporations, and governmental agencies around the world were connected to

ARPANET. ARPANET expired in 1989, but the Internet remained. Federal support for Internet backbones was phased out (except for vBNS, restricted to scientific uses); private commercial providers such as UUNET and Sprint have taken over the Internet backbone business. Today, over 40 million people are connected to the Internet, almost entirely over private or university networks, and the number is expected to grow to over 200 million by the end of the century.

Other computer networks, such as bulletin boards, have sprung up. A bulletin board is a conference and message exchange system usually devoted to a particular topic. The board is operated from a personal computer with one or more modems connected to it. Users access the service by dialing it on their own modems. Commercial online services like Prodigy, CompuServe, and America Online constitute yet another type of computer network.

One primary reason networks like the Internet have grown as fast as they have is freedom from regulation. Computer equipment manufacturers and designers were never burdened with the archaic regulatory structures all too familiar to telephone companies and broadcasters. Competition was fierce. Costs were forced down, making switches, servers, and software cheap enough to permit fast growth. The technology leapt ahead. And the network was simple to hook up to, because the engineers were free to make it so. They were not forced to design content controls or any other social policy into the network. That kept it cheap, and kept it growing.

From that foundation of economic liberty sprang powerful instruments of political freedom and free speech. Those include electronic mail (e-mail), the speedy equivalent of post office mail in the nonelectronic world. Discussion groups such as the "listserv" allow users to subscribe to a list devoted to discussion of a particular topic; any message posted to the list is distributed automatically to other users, usually without being reviewed by a human moderator. Newsgroups are another important forum; they permit users to access information at any time, without a subscription. Information can also be distributed using a home page on the World Wide Web, to which other documents on the Web can be linked. Yet another popular form of computer network speech is the chat room, an electronic forum set up to admit a limited number of speakers. Chats take place in real time and are spontaneous, like a face-to-face chat around a backyard barbecue.

For the ordinary person, computer networks are not just a source of information. They are a source of listeners and readers and viewers.

They transform the ordinary person into a speaker capable of reaching an audience of millions. Computer networks are nothing less than a vast engine of free speech with the potential to transform the entire "marketplace of ideas."

Computer networks can transform markets for goods and services as well. For many commercial and banking transactions, and in the areas of medicine and education, computer communications can substitute for ventures onto crowded highways. Unfortunately, computer networks also can provide new sites for crime. But overreacting to the perceived danger of crime on the net could kill the online commerce goose before it lays any golden eggs. Perhaps the greater danger, however, is that the government will leverage regulation of the network infrastructure into a system that allows it to invade our privacy at will.

The Communications Decency Act and Possible Successors

The Communications Decency Act (CDA), passed as part of the Telecommunications Act of 1996, criminalizes the use of any computer network to display "indecent" material, unless the content provider uses an "effective" method to restrict access to that material to people over the age of 18.

Two panels of judges, convened in New York and Philadelphia, have found there is *no* affordable, effective way for nonprofit or small business providers to restrict children's access to such material. Even if services like credit card authorization were much cheaper and were available for noncommercial transactions, however, the content providers would lose their audiences. No one will cruise the Web if he has to enter a personal identification number or credit card number every time he moves from one Web page or chat room to another. No one is going to bother to obtain a PEN or give his credit card number to view a handful of amateur photos or poems. Even large commercial sites would be affected by the decrease in traffic. *Thus, the statute effectively bans much speech from the Internet and other networks.* Proposed amendments to the statute that would revise it to cover only material that is "harmful to minors" would not substantially improve matters.

The Internet promised the ordinary citizen a low-cost method of reaching an audience beyond immediate family, friends, and neighbors. Legislation like the CDA betrays that hope and is also clearly unconstitutional.

Indeed, no regulation of computer network indecency, however carefully tailored, should pass constitutional scrutiny. Content control is not within the federal government's enumerated powers. And no legislator has been

able to define indecency coherently. Such regulation is inherently unfair, especially as applied to spontaneous, casual speech of the sort that the Internet facilitates between unsophisticated and noncommercial speakers.

Finally, the federal government cannot legitimately claim that it has any interest in content control, when civil society has solved the perceived problem on its own. Private-sector solutions include both software filters that parents can use to screen out offensive material and Internet service providers who provide access only to child-safe materials.

One proposed amendment to the CDA that Congress should reject would have the effect of making the site-rating labels that work with filters such as SurfWatch mandatory for many sites. Mandatory labeling is forced speech. And labeling will not work at all with the most casual, spontaneous computer speech, including e-mail and individual statements posted to newsgroups, lists, and chat rooms. Also, making labeling mandatory will result in labels being applied carelessly or under protest. Voluntary systems will be more carefully administered, and therefore more helpful to parents who want to restrict their children's access to sexually oriented or violent materials.

Congress should repeal the Communications Decency Act and reject all proposed substitutes. The federal government has no legitimate interest in regulating sexually oriented material on the Internet.

Encryption and the First Amendment: Export Controls

Encryption software uses a code to scramble bits of the data sent over computer networks, so that only those with the key to the code can decipher it. The key is a string of numbers. The longer the string, the harder it is to break. The standard key length today is 56 bits. Stronger encryption technology is essential if citizens are to preserve their privacy and security when using computer networks. Otherwise, medical records, credit card numbers, trade secrets, and personal communications relayed over computer networks are not safe from prying eyes. A working group of respected cryptographers recently announced that 56-bit keys are insecure and that keys of at least 90 bits are required to secure information for the next 20 years.

Currently, regulations promulgated under the Arms Export Control Act and the International Emergency Economic Powers Act, as well as the International Traffic in Arms Regulations, hold back the use of strong encryption. There are no restrictions on the domestic use of strong encryption technology, but until recently, encryption software that uses a

key length of more than 40 bits could not be exported without special permission. In the fall of 1996 the Clinton administration announced that it would allow companies to export key lengths of up to 56 bits, under licenses reviewed every six months, if the companies agreed to produce key recovery plans within two years. After two years, nothing stronger than 40 bits will be exportable without key recovery features.

Export controls interfere with the marketing and sale of powerful encryption technology. Software makers must develop one product for sale nationally and another for sale internationally, which is often prohibitively expensive. In developing a product for international sale, they must choose between two unpalatable and unprofitable options. The first is to sell a product internationally that offers only weak cryptographic protection. The second is to sell (or try to sell, after lengthy delays in the licensing process) a product that forces key recovery on their customers. Export controls have severely hampered U.S. software companies' serving world markets for encryption software.

Export controls violate the First Amendment. The export controls sometimes require academic research papers, discussions clearly protected by the First Amendment, that discuss ideas about cryptography to be submitted to the government for review. And, as one court recently held, software expresses ideas in language and is also protected by the First Amendment. No other holding would have made sense; a source code printed in a book is clearly protected by the First Amendment—the same source code stored on a computer disk should be equally protected. Because of export controls, some professors refuse to allow foreign students to take their classes, fearing reprisals from International Traffic in Arms enforcers.

The theory behind export controls is that they prevent strong encryption from falling into the hands of terrorists and criminals. But export restrictions will not keep strong encryption out of the hands of evildoers, since the technology is already widely available. If U.S. companies are forbidden to satisfy the worldwide demand for encryption, companies based in other countries will. A determined organization could, with the aid of a community of mathematicians, develop its own system of encryption using published mathematical models.

Finally, as computers become faster, codes that use keys of 56 bits or even 75 bits will become much easier to break. Software companies should feel free to develop encryption technology as strong as the industry needs. A communication encrypted today might need to remain private for years to come.

Encryption export controls should be lifted. Restricting the mass of users to keys of short bit length merely makes the network insecure; if a code can be broken by law enforcement personnel, it can be broken by hackers.

Encryption and the Fourth Amendment

At the time the Constitution of the United States was written, a group of people could enjoy a completely private conversation by going to the middle of a plowed field, where they could be certain that no one could overhear them. Today, electronic eavesdropping methods allow law enforcement officers to invade even that zone of privacy. New encryption technology will let privacy catch up, although no encryption technology is totally foolproof.

Under mandatory key recovery proposals, encryption software could not be used (either at home or abroad) unless arrangements were made that would enable either the government or a third party to access or reconstruct a key that would decode the message. Encryption without government access to keys would either be outlawed completely or made much less convenient to use. For example, use of public key cryptography often requires a "certification authority." The certification authority is a third party who certifies that the user of a certain public key is in fact a certain individual. Sometimes, the certification authority might be a government agency. Government agencies could refuse to certify the identities of people who would not give access to their private keys.

Such mandatory key access proposals should be rejected. First, the federal government has no constitutional authority to require key access. Imagine a law requiring citizens to escrow their house keys with a third party, so that the police could enter their homes if necessary. Clearly, the Fourth Amendment requires that a warrant be issued on probable cause before the government is entitled to obtain the key to someone's house. There is no exception to the Fourth Amendment for locks that are difficult to pick. Demands for mandatory key escrow constitute an unprecedented power grab on the part of law enforcement officials. The police have always had rights, limited by the Fourth Amendment, to intercept private communications and read them, *if they could.* The police have never had the right to demand that people change the language in which they communicate to make themselves easier to understand.

Second, the security of a cryptographic system rests on the security of the keys, especially the keys used for signatures and identity authentication.

Requiring secret keys to ever leave their users' secure environment endangers the security of the network. So does the collection of large data banks of sensitive key information. Furthermore, third-party storage of private keys is incompatible with super-secure techniques intended to prevent the theft of keys, such as "perfect forward secrecy." And no one understands exactly how key access plans will work; uncertainty about the security of such systems will slow the development of electronic commerce and distort the development of software.

Third, the argument that mandatory key recovery is necessary for data recovery is a pretext. Individuals and firms should decide whether they would prefer a system in which lost keys mean lost data or one in which keys can be recovered. And keys used only for conversations communicated instantaneously need not be stored anywhere. Finally, a system in which keys are stored by a third party is unlikely to be useful for data recovery. Elaborate procedures would be necessary to ensure that the user was indeed entitled to recover the key.

Finally, the gains to law enforcement and national security from key recovery would be minimal. Criminals and terrorists could use multiple encryption to defeat the system; the outer encryption layer would use key recovery, to avert suspicion. The inner layer would not.

Congress should reject attempts to impose key recovery or similar schemes on users of encryption technology.

Conclusion

One of the most common reasons for which people give up their precious civil liberties is fear. Fear of new technology like the Internet is often born of misinformation. There is no more reason for a citizen of the United States to fear the Internet than to fear a printing press or a pen. Information is still information, however it is transmitted. And the First Amendment and the Fourth Amendment remain two important guardians of our civil liberties.

Suggested Readings

Bernstein, Solveig. "Beyond the Communications Decency Act: Constitutional Lessons of the Internet." Cato Institute Policy Analysis no. 262, November 4, 1996.

Corn-Revere, Robert. "New Age Comstockery: Exon vs. the Internet." Cato Institute Policy Analysis no. 232, June 28, 1995.

Key worth, G. A. n, and David E. Colton. "The Computer Revolution, Encryption and True Threats to National Security." *Future Insight,* June 1996.

National Research Council. *Cryptography's Role in Securing the Information Society.* Washington: National Academy Press, 1996.

Post, David. "'Clarifying' the Law of Cyberspace." *American Lawyer,* April 1996.
Samuelson, Pam. "Legally Speaking: The NII Intellectual Property Report." *Communications of the ACM* 37 (December 1994).

—Prepared by Solveig Bernstein and Lawrence Gasman