2000

Cybercrimes v. Cyberliberties

Nadine Strossen
New York Law School

INTERNATIONAL REVIEW OF LAW COMPUTERS
& TECHNOLOGY, VOLUME 14, NO. 1, PAGES 11–24, 2000

Cybercrimes v. Cyberliberties[1]

NADINE STROSSEN[2]

ABSTRACT *The broad topic of 'crime and cyberliberties' encompasses two major subtopics: firstly, the extent to which online expression may be punished under new criminal laws, even if it would be lawful in the traditional print media; and secondly, the extent to which online privacy may be restricted to facilitate enforcement of existing criminal laws. In both contexts, many law enforcement officials argue that we have to make trade-offs between, on the one hand, individual rights and, on the other hand, public safety. In fact, though, the alleged dichotomy is oversimplified and misleading. Claims about the alleged unique dangers of online expression are exaggerated, and the types of criminal laws and law enforcement strategies that have worked effectively in other media are also effective in cyberspace. For example, children should be protected from exploitation in the production of child pornography through the same measures, regardless of whether the material is distributed through postal mail or e-mail. Indeed, individuals and organizations who are devoted to protecting children from exploitation and abuse—whether for the production of child pornography or any other purpose—have expressed frustration that resources that should be used to enforce existing laws are being diverted toward efforts to create new cyberspeech crimes, such as the two US laws criminalizing online material that is 'indecent,' 'patently offensive', or 'harmful to minors'. The many judges who have ruled on these laws—including the entire US Supreme Court—have agreed that they violate free expression rights and are not necessary for their stated purpose of protecting children. The battle to preserve online privacy has not been as successful in the US, where the government restricts strong encryption despite the vigorous objections of not only cyberlibertarians, but also the business community. Moreover, even some law enforcement and other government officials have concluded that, on balance, security concerns are aided, not undermined, by strong encryption, since it protects innocent individuals and legitimate businesses from cybercriminals, and it also protects governments and vital infrastructures from cyberterrorism. Most governments apparently recognize these facts since they have not joined the US in restricting encryption technology.*

Correspondence: Nadine Strossen, New York Law School, 57 Worth Street, New York, NY 10013, USA.

ISSN 1369-0869 Print; 1364-6885 Online/00/010011-14

Introduction

I am delighted and honoured to address this important conference. I want to thank the members of the Cyberlaw Research Unit at the University of Leeds not only for organizing this conference and inviting me to participate in it, but also for their pathbreaking work on cyberlaw and cyberliberties. They have been wonderful colleagues of mine and of the American Civil Liberties Union (ACLU) in both scholarly and advocacy endeavours.

I am proud that the ACLU, which is America's largest and oldest civil liberties organization, has been at the forefront of the newest civil liberties frontier, in cyberspace—not only throughout the US, but also, in collaboration with other organizations around the world, on a global basis. We are spearheading an international coalition called the Global Internet Liberty Campaign, or 'GILC'.[3] And a couple of our most active, effective coalition partners are in Britain and Ireland, including Cyber-Rights & Cyber-Liberties (UK),[4] which was founded by Yaman Akdeniz of the Leeds Cyberlaw Unit. In this international conference, it is important to stress the international scope of our cyberliberties work. Of course, cyberspace is an inherently global medium. And cybercrime and terrorism are worldwide concerns. Likewise, though, preserving human rights in cyberspace is also an international concern.

I have been asked to discuss the legal developments in the US, where we have had more legislation and litigation in this area than any other country. Our courts' rulings have been grounded specifically on US law—in particular, the free speech guarantee of the First Amendment to our Constitution and our constitutional right of privacy. However, those same freedoms are also guaranteed under international human rights law, under regional human rights instruments, including the European Convention on Human Rights, and under the domestic law of nations around the world.[5] Therefore, the principles that have guided legal developments in the US should be relevant in the British Isles and elsewhere, just as developments in Britain and in other parts of the world are also relevant in the US.

Overview of the Interrelationship between Cybercrime and Cyberliberties

The conference organizers asked me to outline the interrelationships between cybercrime and cyberliberties. This broad subject encompasses two major subtopics: first, the extent to which the exercise of certain liberties—notably, free expression—may be criminalized online even if it would be lawful in the traditional print media; and second, the extent to which online liberties—notably, privacy—may be restricted to facilitate punishment of established crimes, such as trafficking in child pornography or engaging in information terrorism. In other words, the first subtopic concerns whether government may restrict our cyberliberties in order to create new crimes, peculiar to cyberspace; and the second concerns whether government may restrict our cyberliberties in order to prosecute existing crimes, common to all media, more effectively.

In both contexts, many officials argue that we have to make trade-offs between, on the one hand, individual rights and, on the other hand, public safety. In fact, though, this alleged tension is oversimplified and misleading. In terms of advancing public safety, measures that stifle cyberliberties are often at best ineffective, and at worst counterproductive. This doubly-flawed nature of laws limiting cyberliberties shows the sadly prophetic nature of a statement that Thomas Jefferson made to James Madison more than 200 years ago, when these two American founders were corresponding about the Bill of Rights to the

US Constitution. Jefferson warned that 'A society that will trade a little liberty for a little order will deserve neither and will lose both'.[6]

This statement is right on the mark concerning the current debates about cybercrimes and cyberliberties, for several reasons. First, claims about the alleged unique dangers of online expression are exaggerated. Second, the types of criminal laws and enforcement strategies that have worked effectively in other media are also effective in cyberspace. Third, far from harming minors, much of the online expression that has been targeted for censorship is affirmatively beneficial for them.

For these reasons, even those who specialize in protecting young people from sexual exploitation and violence—indeed, especially those experts—oppose Internet censorship. This is true, for example, of Ernie Allen, the Director of the National Center for Missing & Exploited Children in the US, which works closely with the Federal Bureau of Investigation and local police agencies around our country. Mr Allen and his colleagues understand that the political obsession with suppressing ideas and images that are allegedly harmful to children's minds is a dangerous distraction and diversion from constructive efforts to protect actual children from tangible harm.[7] In short, cybercensorship does no more good for the safety and welfare of young people than it does for the free speech rights of everyone—and I say 'everyone' advisedly, since young people have free speech rights of their own.[8]

The same false tension between liberty and security also marks too much of the political rhetoric about protecting online privacy through such measures as strong encryption or cryptography and anonymous communications. To be sure, law enforcement would to some extent be aided if officials could easily gain access to online communications, just as law enforcement would receive some benefits if officials could readily spy on all communications of any type. But such pervasive surveillance would violate internationally respected, fundamental privacy rights.[9] The consensus of the international community is that this would be too high a price to pay for reducing crime. After all, what would be the point of limiting our fellow citizens' interference with our personal security, only at the price of increasing police officers' interference with the very same security?[10] This point was eloquently stated by a great former Justice of the US Supreme Court, Louis Brandeis, who was one of the architects of the legal right to privacy even before he ascended to the high Court.[11]

> Decency, security and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen ... . Our Government is the potent, the omnipresent teacher ... . Crime is contagious. If the Government becomes a lawbreaker it breeds contempt for law ... . To declare that in the administration of the criminal law the end justifies the means—... that the Government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution.[12]

Just as weakened privacy protections would let government officials access online communications by ordinary, law-abiding citizens, these same weakened protections would also enhance access to online communications by cybercriminals and terrorists. They will not comply with government restrictions on encryption. To the contrary, they will take all available measures to secure their own communications, including illegal measures. Meanwhile, thanks to legal limits on encryption, cybercriminals will more easily prey on law-abiding individuals and businesses, and vital infrastructures will be more vulnerable to cyberterrorists. For these reasons, even some government officials have joined with cyber-

libertarians in opposing limits on encryption. They concur that, on balance, such limits do more harm than good to public safety.[13]

That, in a nutshell, is my broad overview of the relationship between cyberliberties and crime control: namely, that this relationship, far from being inherently antagonistic, is often mutually reinforcing. In many respects, law and public policy are developing in a way that is consistent with this perspective. In the US, the courts consistently have struck down new laws that seek to criminalize online expression that would be legal in other media. Many judges who have ruled on such laws have agreed with the ACLU and other cyberlibertarians that the laws are not in fact well-designed for protecting children, which is their asserted goal. These judges include the entire US Supreme Court, ruling in the landmark 1997 case striking down the first federal Internet censorship law in the US, the Communications Decency Act, or 'CDA',[14] in *Reno* v. *ACLU*.[15]

Now we have to call that case *ACLU* v. *Reno I*, since the US federal government recently enacted its second cybercensorship law, the so-called 'Child Online Protection Act' or 'COPA',[16] which we are now fighting in a case called *ACLU* v. *Reno II*.[17] With a name like the 'Child Online Protection Act', it is not surprising that few politicians had the political courage to oppose this law. Fortunately, though, the only judge to rule on the law to date has agreed with us that it is not only unconstitutional, but also unwise and misnamed since it does not really protect children. Indeed, he concluded his opinion on this note: '[P]erhaps we do the minors of this country harm if First Amendment protections, which they will with age inherit fully, are chipped away in the name of their protection.'[18]

When we turn from online free speech to privacy, the US courts have likewise been supportive of our arguments that restricting cyberliberties cannot be justified in terms of the alleged countervailing law enforcement concerns. For example, in *ACLU* v. *Miller*,[19] we successfully challenged a state law that prohibited anonymous and pseudonymous online communications. There have, though, been fewer rulings concerning privacy than free speech in the online context, they have only been issued by lower-level courts, and they have not been as consistently supportive of the cyberliberties positions.[20]

In the US, the battle over online privacy and encryption is being waged mostly in the legislative and executive branches of government, rather than in the courts, with the Clinton Administration steadily opposing strong encryption, but with many members of Congress, from both major political parties, on the other side. Thus far, at least, the US government is quite isolated in the international community in this respect, since most other countries allow strong encryption.[21] That is certainly true in Europe, which in general has stronger legal protections for privacy of communications and data than we have in the US.[22] However, the Clinton Administration is working hard to export its anti-privacy, anti-encryption stance around the world,[23] and it has gained support from some officials here in Britain, for example. Therefore, it is essential to understand why this stance is as inimical to public safety as it is to personal privacy.

Criminalizing Sexually-Oriented Online Expression

Now that I have sketched out the general picture concerning the relationship between cyberliberties and cybercrime, I would like to spend the rest of my time filling in some of the details. Let me start with the area where we have had the most legislation and litigation in the US, since this is also an area of great concern in other countries, including right here in Britain: namely, criminalizing online expression that is sexually oriented. In fact, Yaman

Akdeniz and I are co-authoring a book chapter on this topic, focusing on this aspect of cyberlaw in both the UK and the US.[24]

In the US, from the moment that cyberspace first hit the public radar screen, we immediately saw political and media hysteria about 'cyberporn' and efforts to censor online expression of a sexual nature. This reaction was not surprising. Despite Americans' general commitment to free speech, throughout our history, any sexually-oriented expression in any medium has always been suspect. That is because of my country's Puritanical heritage—which, of course, we share with the British Isles. One of America's most popular humorists, Garrison Keillor, put it this way: 'My ancestors were Puritans from England [who] arrived in America in 1648 in the hope of finding greater restrictions than were permissible under English law at the time.'[25] Consistent with this long-standing American tradition, we are seeing many efforts to stifle online sexual expression, all over the US, at all levels of government, from the US Congress and Clinton Administration to local school boards and library boards.[26] From a free speech perspective, that is the bad news about sexually-oriented expression online.

But there is good news too. Just as elected officials have mostly supported censorship of sexually-oriented online material, the courts have provided a welcome contrast, as I have indicated. So far, the ACLU has brought constitutional challenges to seven new laws censoring sexually-oriented material online: the two federal statutes I already mentioned;[27] four state laws (in New York,[28] Virginia,[29] New Mexico[30] and Michigan[31]); and one local law (in Loudoun County, Virginia[32]). And so far, we have won every single one of these challenges, with only one recent exception, which I do not think is too significant for cyberliberties (as I will explain in a moment). Moreover, these decisions affirming freedom of cyberspeech have been joined in by 19 different judges who span a broad ideological spectrum, having been appointed by the last six US Presidents, going all the way back to Richard Nixon (including four Republicans and two Democrats). In short, the ACLU position on online free speech is essentially the position that is now enshrined in First Amendment law.

The one recent setback is an intermediate appellate court ruling on a Virginia state law restricting government employees' access to sexually-oriented online material.[33] The US Supreme Court has held that the government, when it acts as employer, may impose more limits on its employees' expression than the government, when it acts as sovereign, may impose on its citizens' expression.[34] Nevertheless, the lower court agreed with us that Virginia's law violated even the reduced free speech rights of government employees.[35] In contrast, the intermediate appellate court overturned that decision in February, 1999 on the broad rationale that government employees have no free speech rights concerning any communications in any medium whenever they act primarily in their role as employees.[36] So, this court was not imposing special restrictions on expression in cyberspace as opposed to other media. Rather, it was imposing special restrictions on expression by government employees, regardless of the medium. We think this ruling was wrong, and hope to overturn it on further appeal. In any event, though, it really does not have any special impact specifically on *cyber*law or *cyber*liberties.

In contrast, our two most recent victories in cybercensorship cases do have broad positive implications for online free speech, so I would like to describe those. First, let me tell you a bit more about our lower court victory in February, 1999 in *ACLU* v. *Reno II*, against the second federal cybercensorship law, COPA. In response to the Supreme Court's decision striking down the CDA in *ACLU I*,[37] Congress wrote a somewhat less sweeping law the second time around. The CDA had criminalized any online expression that is

'patently offensive'[38] or 'indecent'.[39] In contrast, COPA outlaws any online communication 'for commercial purposes'[40] that 'includes any material that is harmful to minors'.[41] Both of COPA's critical terms are defined broadly. First, a communication is 'for commercial purposes' if it is made 'as a regular course of ... trade or business, with the objective of earning a profit', even if no profit is actually made.[42] Therefore, COPA applies to many not-for-profit Websites, which provide information completely free—including the ACLU's own Website. Second, material is 'harmful to minors' if it satisfies US law's three-part obscenity definition specifically as to minors—namely, if it appeals to the prurient interest in sex, is patently offensive, and lacks serious value, from a minor's perspective.[43]

I should note that the ACLU opposes the obscenity exception that the US Supreme Court has carved out of the First Amendment (over the dissenting votes of many respected Justices).[44] However, we have not used our cybercensorship cases as occasions for challenging that exception. In other words, we have not challenged these new laws to the extent that they simply transplant to cyberspace existing free speech exceptions, which have been upheld in other media—in particular, obscenity, child pornography, and solicitation of a minor for sexual purposes. Rather, what we have actively opposed in these new laws is their creation of new, broader categories of expression that is unprotected specifically online, even though it would be constitutionally protected in traditional print media. So, with that perspective, let me turn back to *ACLU* v. *Reno II*. On 1 February 1999, a federal judge, Lowell Reed, granted our motion for a preliminary injunction.[45] He enjoined the government from enforcing COPA pending the trial on the merits. Judge Reed held that we had shown the necessary 'likelihood of success' on the merits of our claim that COPA violates the First Amendment for many of the same reasons that CDA did.

Since COPA regulates expression that is protected 'at least as to adults',[46] Judge Reed ruled, it is presumptively unconstitutional unless the government can satisfy the demanding 'strict scrutiny' test. It has to show both that the law's purpose is to promote an interest of 'compelling' importance and that the law is narrowly tailored to promote that purpose—in other words, that there are no 'less restrictive alternative' measures, which would be less burdensome on free speech.[47] Judge Reed concluded that the government does have a compelling interest in shielding minors even from materials that are not obscene by adult standards.[48] However, Judge Reed also concluded that the government was unlikely to be able to show that COPA is the least restrictive means of achieving this goal.[49] For example, Judge Reed noted that the evidence before him 'reveals that blocking or filtering technology may be at least as successful as COPA would be in restricting minors' access to harmful material online without imposing the burden on constitutionally protected speech that COPA imposes on adult users or Web site operators'.[50] The government has appealed from Judge Reed's ruling.[51] Quite likely, this case will go all the way to the US Supreme Court, which has only issued one decision on the 'harmful to minors' doctrine, which was more than 30 years ago.[52]

Now let me turn to our second recent victory, in another important cyberspeech case, which is also still working its way through the court system. This case is called *Mainstream Loudoun* v. *Loudoun County Library*,[53] and it is so far the only court ruling on the burgeoning controversy over filtering and blocking software. Ever since it became clear that the CDA and other direct censorial measures were facing constitutional difficulties, advocates of suppressing online sexual expression stepped up their promotion of rating and filtering systems, which would also bar access to the same expression. The ACLU has issued two reports explaining why all these systems are problematic for many reasons.[54]

For one thing, the filtering software is inevitably both under-inclusive and over-inclusive, in terms of blocking all the material it purports to, and only that material. Therefore, while individual Internet users certainly have the right to install software on their own computers that blocks out material they consider contrary to their values, there is still a problem. Almost all manufacturers of blocking software refuse to disclose either the sites they block or the criteria they use to determine which sites they will block. Consequently, the manufacturers are imposing their value choices on their customers. They are not facilitating the customers' exercise of their own freedom of choice. In short, this is really more of a consumer protection problem than a free speech problem. However, there is a serious free speech problem when the filtering software is installed not as a matter of choice on the part of individual users, but rather, by government officials who control the computers—in public institutions. Across the US, officials are busily installing or advocating blocking software on computers in public libraries, schools, and universities.[55] Therefore, individual choice is stripped from the many members of the public whose only access to the Internet is through such computers. For them, the installation of filtering software on, say, library computers has the same censorial impact as the removal of books from library shelves. And book banning is precisely the analogy that was invoked by the only court that has ruled on this issue to date. In November 1998, federal judge Leonie Brinkema upheld a First Amendment challenge to mandatory filtering software that had been installed in the Loudoun County, Virginia public libraries.[56] Pursuant to a 'Policy on Internet Sexual Harassment', the library officials required software to block 'child pornography and obscene material', as well as material deemed 'harmful to juveniles' under state law.[57]

As an aside—but an important one—I want to note the distorted, overbroad concept of sexual harassment that is reflected in this policy, along with too many others. The policy assumes that the presence of sexually oriented expression on library computer terminals *ipso facto* constitutes illegal sexual harassment. But that assumption is patently incorrect. As the US Supreme Court has held, expression does not give rise to a sexual harassment claim merely because a person at whom it is directed considers it offensive.[58]

Even beyond the library's misguided concept of sexual harassment, it also implemented its policy in a way that violated online First Amendment rights, and that was the focus of Judge Brinkema's ruling. Specifically, the library installed a commercial software product called 'X-Stop'. Judge Brinkema held that the filtering requirement operated as a presumptively unconstitutional 'prior restraint' on expression. Therefore, it had to withstand the same type of strict judicial scrutiny that has also been applied to other censorial laws, such as CDA and COPA.[59]

Judge Brinkema assumed for the sake of argument that the government's asserted interests were of compelling importance—namely, its interests in minimizing access to obscenity and child pornography, and in avoiding the creation of a sexually hostile environment.[60] However, Judge Brinkema concluded that the blocking policy was unconstitutional on several, independently sufficient, grounds: (1) it is not necessary to further the government's asserted interests; (2) it 'is not narrowly tailored'; (3) it limits adult patrons to accessing only material that is fit for minors; (4) it 'provides inadequate standards for restricting access'; and (5) it 'provides inadequate procedural safeguards to ensure prompt judicial review'.[61]

One particularly interesting feature of Judge Brinkema's analysis is her catalogue of 'less restrictive means' that Loudoun County could have used to pursue its asserted interests: installing privacy screens; charging library staff with casual monitoring of Internet use; installing filtering software only on some Internet terminals, and limiting minors to those

terminals; and installing filtering software that could be turned off when an adult is using the terminal.[62] Significantly, Judge Brinkema cautioned that while all of the foregoing alternatives are less restrictive than the challenged mandatory filtering policy, she did not 'find that any of them would necessarily be constitutional', since that question was not before her.[63] Loudoun County officials decided not to appeal from Judge Brinkema's ruling.[64] Of course, the constitutional questions involved will not be settled until the US Supreme Court rules on them in another filtering controversy.[65]

Debates about Online Privacy and Cryptography

In the following sections, I would like to amplify a bit on the second major aspect of the cyberliberties/crime debate that I outlined earlier: the controversy about online privacy and encryption or cryptography. Advocates of restricting encryption argue that, as the price for barring criminals and terrorists from using effective cryptography, we must also bar law-abiding citizens and businesses from doing so. This rationale was effectively debunked in an excellent report that Cyber-Rights and Cyber-Liberties (UK) issued in September 1998 and entitled 'Cyber-crime and Information Terrorism'[66]: 'Many things are valuable to criminals and terrorists but this alone does not provide a reason for imposing controls .... [C]riminals find cars useful but society doesn't control the supply of cars because of this.'[67]

In light of this passage, it is ironic to note that when the automobile was first invented, law enforcement officials did seek to restrict its usage, precisely because they did fear that it would facilitate criminal activities.[68] Today that argument seems ludicrous, but, at bottom, it is precisely the same as the one that is now being offered in an attempt to justify restrictions on cryptography. This is the argument that is being made by the Clinton Administration in the US. The Clinton Administration insists that the only kind of encryption technology that should be available is 'key recovery' or 'key escrow' cryptography. Yet this type of encryption is inherently insecure, since it is expressly designed to give covert access to the plaintext of encrypted data to a third party—in particular, the government.

Although some government officials contend that there is a conflict between cyberliberties and cybercrime or cyberterrorism, in fact, that is not so. To the contrary, this situation vividly illustrates Thomas Jefferson's observation I previously quoted: about liberty and security concerns working in tandem, rather than in tension, with each other. Indeed, it is particularly apt to refer to Jefferson's communications with Madison in the cryptography context; when these two American founders corresponded prior to the signing of the Declaration of Independence, they encoded all their messages—in short, they used 18th-century-style encryption![69] Notwithstanding the Clinton Administration's adamant official position, individual officers and agencies in the US government have broken ranks. One important example is a high-level US government committee: the National Research Council (NRC) committee on cryptography. In its 1996 report, this committee concluded that strong encryption is essential for promoting law enforcement and national security:

> If cryptography can protect the trade secrets and proprietary information of businesses and thereby reduce economic espionage (which it can), it also supports in a most important manner the job of law enforcement. If cryptography can help protect nationally critical information systems and networks against unauthorized penetration (which it can), it also supports the national security of the United States.[70]

Accordingly, even though this NRC report recognized that restricting encryption would strengthen some law enforcement efforts, it nevertheless concluded that '[o]n balance, the advantages of more widespread use of cryptography outweigh the disadvantages'.[71] Some of the reasons for this conclusion were outlined as follows in a September 1998 GILC report that focused specifically on the precise type of cryptography regulation that has been enforced and advocated by the US—export restrictions:

> [E]xport controls on cryptography hurt law-abiding companies and citizens without having any significant impact on the ability of criminals, terrorists or belligerent nations to obtain any cryptographic products they wish;
> [E]xport restrictions imposed by the major cryptography-exporting states limit the ability of other nations to defend themselves against electronic warfare attacks on vital infrastructure;
> [F]ailure to protect the free use and distribution of cryptographic software will jeopardize the life and freedom of human rights activists, journalists and political activists all over the world;
> [A]ny restriction on the use of cryptographic programs will be unenforceable in practice, since the basic mathematical and algorithmic methods for strong encryption are widely published and can easily be implemented in software by any person skilled in the art;
> [T]he increasingly common use of public networks to electronically distribute such products in intangible form reinforces the unenforceability of export controls.[72]

For the foregoing reasons, restrictions on encryption are not even effective, let alone necessary, in countering cybercrime. On this ground alone, such restrictions should be rejected. But there are also additional grounds for this conclusion. For one thing, the government cannot show that there is in fact a substantial danger of the specific type of crime that is claimed most urgently to warrant restrictions on cryptography—namely, information terrorism. Fortunately, claims about this potential problem turn out to be greatly overblown. This was shown, for example, by a recent study, published in the Fall 1998 Internet publication, *Issues in Science and Technology Online*. Its title effectively summarizes its conclusion: 'An Electronic Pearl Harbor? Not Likely'. The study was written by George Smith, an expert on computer crime, security and information warfare.[73] He dismissed government and media descriptions of the dangers of cyberterrorism as 'myths',[74] 'hoaxes'[75] and 'the electronic ghost stories of our time'.[76] Although the Smith study focused on the US, no doubt it is relevant for other countries too. Here is its conclusion:

> The government's evidence about U.S. vulnerability to cyber attack is shaky at best. ... Although the media are full of scary-sounding stories about violated military Web sites and broken security on public and corporate networks, the menacing scenarios have remained just that—only scenarios. ... [An examination of the] sketchy information that the government has ... provided ... casts a great deal of doubt on the claims.[77]

Precisely the same conclusion was reached by a report by a commission appointed by President Clinton on 'Critical Infrastructure Protection'.[78] The Commission was charged with analysing the danger that information terrorists could pose to our nation's infrastructure—communications lines, power grids and transportation networks. The Commission's members consisted largely of military and intelligence officials. Therefore, the Commission was, presumably, especially sympathetic toward government claims of law enforcement and national security threats. Yet even this group was forced to acknowledge that there was

no evidence of an 'impending cyber attack which could have a debilitating effect on the nation's critical infrastructure'.[79]

Nonetheless, that recognition did not deter the commission from seizing upon the fear of cyberterrorism to press for government measures that constrict individual rights, including key recovery encryption. Indeed, the Commission was so eager to leverage public concerns about info-terrorism into heightened government surveillance over the public, that it disregarded the countervailing dangers that key recovery encryption poses to the very infrastructure that the Commission was created to protect![80] Those dangers were well-described, for example, in the recent report by Cyber-Rights & Cyber-Liberties (UK), on 'Cyber-crime and Information Terrorism':

> Increasingly, the economies of the developed and developing nations are dependent on networked computing resources. Irrespective of whether it is communications, electrical power generation, road, rail or air transport, stock exchanges, banks, finance houses, agriculture, hospitals or a host of other infrastructures, all now depend on regular and continuous information exchanges between networked computer systems for their continuing safe operation. In the absence of effective cryptographic protection the computer systems that keep these infrastructures operating are wide open to attacks by terrorist and criminal organizations using only modest resources. Cryptographic ... controls are preventing the protection of these civil infrastructures and rendering them easy and tempting targets for international terrorists and criminals. Far from impeding crime and terrorism, therefore, controls on cryptography are having precisely the opposite impact.[81]

These same dangers had been heralded in a May 1997 report by 'an Ad Hoc Group of Cryptographers and Computer Scientists', 'The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption':

> Any key recovery infrastructure, by its very nature, introduces a new and vulnerable path to the unauthorized recovery of data where one did not otherwise exist. This ... creates new concentrations of decryption information that are high-value targets for criminals or other attackers .... The key recovery infrastructure will tend to create extremely valuable targets, more likely to be worth the cost and risk of attack.[82]

In sum, not only are claims about the dangers of cyberterrorism exaggerated, but also, the proposed counter-measures—notably, restrictions on cryptography—far from being necessary to respond to any such dangers, are not even effective; to the contrary, they are counterproductive.

A number of recent government reports have reached precisely the same conclusions. For example, last September, a European Parliament report called for rejecting encryption controls, including those advocated by the US.[83] Significantly, this report was issued in the wake of increasing evidence of unjustified surveillance by law enforcement agencies in various European countries. Indeed, the vast majority of governments that have considered the issue have opposed restrictions on encryption. This pattern was documented by a comprehensive report that GILC issued in February 1998, entitled 'Cryptography and Liberty'.[84] It surveyed the cryptography policies of all countries in the world, based on direct communications with their governments. It concluded that, in most countries, cryptography may be freely used, manufactured, and sold without restriction. As the GILC report concluded that '[f]or those [countries] that have considered the topics, interests in electronic commerce and privacy ... outweigh the concerns expressed by law enforcement'.[85]

Conclusion

In conclusion, everyone who values human life—and human rights—must of course be vigilant against the fear, insecurity, and manipulation caused by terrorists and other criminals. But we must also be vigilant against the fear, insecurity, and manipulation caused by those who seek to fight against criminals. In a classic 1927 opinion, the great US Supreme Court Justice Louis Brandeis cautioned against ceding our hard-won freedoms to even well-intentioned government agents. Tellingly, that opinion warned against electronic surveillance and restrictions on free speech and privacy with respect to the then-newest communication technology—the telephone—despite claims about the urgent need to fight against telephonic crime. Justice Brandeis's stirring, prophetic words apply fully to electronic surveillance and restrictions on free speech and privacy with respect to the now-newest communication technology—cyberspace—despite claims about the urgent need to fight against cybercrimes and information terrorism. As Justice Brandeis warned:

> Experience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent .... The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.[86]

Notes and References

1 Keynote Address presented to 'Cyberspace 1999: Crime, Criminal Justice and the Internet', 14th BILETA Annual Conference, York, March 29, 1999. For research assistance with this essay, including drafting the footnotes, Professor Strossen gratefully acknowledges her Chief Aide, Amy L. Tenney, and her Research Assistant, César de Castro. The footnotes were added through the efforts of Professor Strossen's staff who thereby have earned both the credit and the responsibility for these notes (which Professor Strossen has not reviewed, and for which she disclaims both credit and responsibility). Finally, she would like to thank the conference organiser Dr David Wall and also Yaman Akdeniz, Cyberrights and Cyberliberties, UK, for inviting her to address the conference.

2 Professor of Law, New York Law School; President, American Civil Liberties Union.

3 Global Internet Liberty Campaign. Online. Available online at < http://www.gilc.org > (21 June 1999).

4 Cyber-Rights & Cyber-Liberties (UK). Available online at < http://www.cyber-rights.org > (2 June 1999).

5 Global Internet Liberty Campaign *Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on the Global Internet*, 1998. Available online at < http://www.gilc.org/speech/report > (20 September 1999); Global Internet Liberty Campaign *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, 1998. Available online at < http://www.gilc.org/privacy/survey/intro.html > (13 September 1999).

6 *Williams* v. *Garrett*, 722 F. Supp. 254, 256 (W.D. Va. 1989) (quoting Thomas Jefferson).

7 N Strossen and E Allen 'Megan's Law and the Protection of the Child in the On-Line Age', *American Criminal Law Review*, Vol 35, pp 1319–1341, 1998. In a related vein, Professor Frederick Schauer of Harvard University testified against the Child Pornography Prevention Act of 1996, a federal law punishing anyone who possesses any work that depicts someone who appears to be a minor engaged in 'sexually explicit conduct'. Schauer stated that the law would '"wind up hurting rather than helping the cause of prosecuting the ... individuals who exploit children" by diverting resources away from actual prosecution of child molesters'. N Strossen *Bang the Tin Drum No More*, 1997. Available online at < http://www.intellectualcapital.com/issues/issue97/item2462.asp > (21 June 1999).

8 *Erznoznik* v. *City of Jacksonville*, 422 US 205, 212 (1975) ('[M]inors are entitled to a significant measure of First Amendment protection.'); *Tinker* v. *Des Moines Indep. Community Sch. Dist.*, 393 US 503, 506 (1969) ('First Amendment rights ... are available to ... students.'); United

Nations Children's Fund *Convention on the Rights of the Child*, 1989. Available online at <http://www.unicef.org/crc/part1.htm > (21 June 1999), Article 13 ('The child shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of the child's choice.').

9 Electronic Privacy Information Center, *Cryptography and Liberty 1999: An International Survey of Encryption Policy*, 1999. Available online at <http://www2.epic.org/reports/crypto1999.html > (24 July 1999), p 8.

10 The concept of the right to privacy as personal security against unwarranted intrusion by others is embodied in many legal guarantees of that right, including the Fourth Amendment to the US Constitution, which provides, in pertinent part: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated ... .' Indeed, many individuals feel particularly threatened by governmental intrusions.

11 S D Warren and L D Brandeis 'The right to privacy', *Harvard Law Review*, Vol 4, p 193, 1890.

12 *Olmstead* v. *US*, 277 U.S. 438, 485 (1928) (Brandeis, J. dissenting), overruled by *Katz* v. *United States*, 389 US 347 (1967).

13 National Research Council *Cryptography's Role in Securing the Information Society*, 1996. Available online at <http://www.nap.edu/readingroom/books/crisis/ > (29 September 1999).

14 47 U.S.C. § 223 (a, d) (1999).

15 *Reno* v. *American Civil Liberties Union*, 521 U.S. 844 (1997).

16 47 U.S.C. § 231 (1999).

17 *American Civil Liberties Union* v. *Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999).

18 *Ibid.* at 498.

19 *American Civil Liberties Union* v. *Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997).

20 *Bernstein* v. *US*, 974 F. Supp. 1288 (N.D. Ca. 1997), *aff'd*,176 F.3d 1132 (9th Cir. May 6, 1999) (holding that encryption regulations were an unconstitutional prior restraint in violation of the First Amendment). *But c.f.*, *Junger* v. *Dale*, 8 F.Supp. 2d 708, 715 (N.D. Oh. 1998) (holding that 'although encryption source code may occasionally be expressive, its export is not protected conduct under the First Amendment'); *Karn* v. *US Department of State*, 925 F. Supp. 1 (D.D.C. 1996) (rejecting First Amendment challenge to encryption export regulations). In mid-September 1999, the Clinton Administration announced that it will relax encryption export controls. J Clausing 'In a reversal, White House will end data-encryption export curbs', *New York Times*, 17 September 1999, C1. However, even with the Clinton Administration's recent pronouncement, civil libertarians continue to point out the problems with encryption regulations—namely, that export control laws on encryption are unconstitutional prior restraints on speech, and that the new proposed regulations apply only to commercial, not academic, work. Electronic Frontier Foundation *Latest Governmental Encryption Scheme Still Unconstitutional: EFF-Sponsored Legal Challenge Will Proceed*, 1999. Available online at <http://www.eff.org/91699_crypto_release.html> (16 September 1999). Shortly before this article went to press, the Ninth Circuit withdrew the three-judge panel decision in *Bernstein* and ordered the case to be reheard *en banc*. *Bernstein* v. *US*, No. 97–16686, 1999 US App. LEXIS 24324 (9th Cir. 30 September 1999).

21 Global Internet Liberty Campaign *Cryptography and Liberty An International Survey of Encryption Policy*, 1998. Available online at <http://www.gilc.org/crypto/crypto-survey.html > (20 September 1999), p 5.

22 *Ibid.* at 5.

23 *Ibid.* at 6.

24 Y Akdeniz and N Strossen 'Obscene and indecent speech' in C Walker, Y Akdeniz and D Wall (eds) *The Internet, Law and Society*, London, Addison Wesley Longman, forthcoming.

25 Garrison Keillor, Statement to the Senate Subcommittee on Education, 29 March 1990 (Testimony on NEA Grant Funding and Restrictions) 136 Cong. Rec. E. 993 (1990).

26 American Civil Liberties Union: Cyberliberties. Available online at <http://www.aclu.org/issues/cyber/hmcl.html > (28 August 1999).

27 *Reno* v. *American Civil Liberties Union*, 521 U.S. 844 (1997); *American Civil Liberties Union* v. *Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999).
28 *American Library Ass'n* v. *Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997).
29 *Urofsky* v. *Allen*, 995 F. Supp. 634 (E.D. Va. 1998), overruled by *Urofsky* v. *Gilmore*, 167 F.3d 191 (4th Cir. 1999).
30 *American Civil Liberties Union* v. *Johnson*, 4 F. Supp. 2d 1029 (D.N.M. 1998).
31 *Cyberspace* v. *Engler*, 55 F. Supp. 2d 737 (E.D. Mich. 1999).
32 *Mainstream Loudoun* v. *Loudoun County Library*, 24 F. Supp. 2d 552 (E.D. Va. 1998).
33 *Urofsky* v. *Gilmore*, 167 F.3d 191 (4th Cir. 1999).
34 *Waters* v. *Churchhill*, 511 U.S. 661, 674–75 (1994); *Pickery* v. *Board of Educ.*, 391 U.S. 563, 568 (1968).
35 *Urofsky* v. *Allen*, 995 F. Supp. 634 (E.D. Va. 1998).
36 *Urofsky* v. *Gilmore*, 167 F.3d 191, 196 (4th Cir. 1999).
37 *Reno* v. *American Civil Liberties Union*, 521 U.S. 844 (1997).
38 47 U.S.C. § 223(d)(1)(B).
39 47 U.S.C. § 223(a)(1)(B)(ii)
40 47 U.S.C. § 231(a)(1).
41 *Ibid.*
42 47 U.S.C. § 231(e)(2)(B).
43 47 U.S.C. § 231(e)(6).
44 N Strossen *Defending Pornography: Free Speech, Sex, and the Fight for Women's Rights*, New York, Scribner, 1995, p 57–58.
45 *American Civil Liberties Union* v. *R eno*, 31 F.Supp. 2d 473 (E.D. Pa. 1999).
46 *Ibid.* at 492.
47 E Chemerinsky *Constitutional Law: Principles and Policies*, New York, Aspen Law & Business, 1997, p 416.
48 *American Civil Liberties Union* v. *Reno*, 31 F.Supp. 2d 473, 495 (E.D. Pa. 1999).
49 *Ibid.* at 497.
50 *Ibid.*
51 American Civil Liberties Union, *Internet Censorship BattleMoves to Appeals Court*, 1999. Available online at <http://www.aclu.org/features/f101698a.html > (28 August 1999).
52 *Ginsberg* v. *New York*, 390 US 629 (1968).
53 *Mainstream Loudoun* v. *Loudoun County Library*, 24 F.Supp. 2d 552 (E.D. Va. 1998).
54 American Civil Liberties Union, *Fahrenheit 451.2: Is Cyberspace Burning?*, 1997. Available online at <http://www.aclu.org/issues/cyber/burning.html > (28 August 1999); American Civil Liberties Union, *Censorship In a Box*, 1998. Available online at <http://www.aclu.org/issues/cyber/box.html > (28 August 1999).
55 American Civil Liberties Union *Censorship In A Box*, 1998. Available online at <http://www.aclu.org/issues/cyber/box.html > (28 August 1999), pp 9–10.
56 *Mainstream Loudoun* v. *Loudoun County Library*, 24 F. Supp. 2d 552 (E.D. Va. 1998).
57 *Ibid.* at 567.
58 *Harris* v. *Forklift Sys. Inc.*, 510 US 17, 21 (1993); N Strossen *Defending Pornography: Free Speech, Sex, and the Fight for Women's Rights*, New York, Scribner, 1995, Chapter 6, pp 119–140.
59 *Mainstream Loudoun* v. *Loudoun County Library*, 24 F.Supp. 2d 552, 564–65 (E.D. Va. 1998).
60 *Ibid.* at 564.
61 *Ibid.* at 570.
62 *Ibid.* at 567.
63 *Ibid.*
64 D Hedgpeth 'Libraries abandon court fight; board won't appeal internet policy rulings', *Washington Post*, 22 April 1999, V03.

65 For detailed information on all of these cases, including the parties' litigation papers and the courts' rulings, see the ACLU's website. American Civil Liberties Union. Available online at <http://www.aclu.org/issues/cyber/hmcl.html > (28 August 1999).

66 B Gladman *Wassenaar Controls, Cyber-Crime and Information Terrorism*, 1998. Available online at <http://www.cyber-rights.org/crypto/wassenaar.htm > (29 September 1999), pp 4–5.

67 *Ibid.*

68 National Public Radio 'Feds say e-mail scrambler is a weapon', National Public Radio Morning Edition, 14 April 1995.

69 J Fraser 'The use of encrypted, coded and secret communications is an 'ancient liberty' protected by the US Constitution', *Virginia Journal of Law and Technology*, Vol 2, p 25, n 123, 1997.

70 National Research Council *Cryptography's Role in Securing the Information Society*, 1996. Available online at <http://www.nap.edu/readingroom/books/crisis/ > (29 September 1999), p 24.

71 *Ibid.* at 27.

72 Global Internet Liberty Campaign *Cryptography is a Defensive Tool, Not a Weapon*, 1998. Available online at <http://www.gilc.org/crypto/wassenaar/gilc-statement-998.html > (30 September 1999), p 2.

73 G Smith *An Electronic Pearl Harbor? Not Likely*, 1998. Available online at <http://www.nap.edu/issues/15.1/smith.htm > (20 September 1999).

74 *Ibid.* at 1.

75 *Ibid.* at 2.

76 *Ibid.* at 9.

77 *Ibid.* at 1.

78 The President's Commission on Critical Infrastructure Protection *Critical Foundations; Report Summary*, 1997. Available online at <http://www.info-sec.com/pccip/web/summary.html > (10 October 1999).

79 A Oram *A Sacrifice to the War Against Cyber-Terrorism*, 1997. Available online at <http://www.oreilly.com/people/staff/andyo/ar/terror _pub.html> (quoting the report issued by the President's Commission on Critical Infrastructure Protection on 13 October 1997 and presented by its Chairman Robert T. Marsh, before a Congressional Committee on 5 November 1997).

80 Electronic Privacy Information Center *White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*, 1998. Available online at <http://www.epic.org/security/infowar/cip _white_paper.html> (20 September 1999).

81 B Gladman *Wassenaar Controls, Cyber-Crime and Information Terrorism*, 1998. Available online at <http://www.cyber-rights.org/crypto/wassenaar.htm > (29 September 1999), pp 4–5.

82 Ad Hoc Group of Cryptographers and Computer Scientists *The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption*, 1998. Available online at <http://www.cdt.org/crypto/risks98 > (29 September 1999), p 15–16.

83 Omega Foundation *An Appraisal of the Technologies of Political Control*, 1998. Available online at <http://www.jya.com/stoa-atpc-so.htm > (8 October 1999).

84 Global Internet Liberty Campaign *Cryptography and Liberty 1998*, 1998. Available online at <http://www.gilc.org/crypto/crypto-survey.html > (29 September 1999). Shortly before this article went to press, EPIC published the 1999 update to this report. Electronic Privacy Information Center *Cryptography and Liberty 1999: An International Survey of Encryption Policy*, 1999. Available online at <http://www2.epic.org/reports/crypto1999.html > (24 July 1999).

85 Global Internet Liberty Campaign *Cryptography and Liberty 1998*, 1998. Available online at <http://www.gilc.org/crypto/crypto-survey.html > (29 September 1999), p 7.

86 *Olmstead* v. *US*, 277 US 438, 479 (1928) (Brandeis, J. dissenting), overruled by *Katz* v. *US*, 389 US 347 (1967).