2009

Cybercrimes vs. Cyberliberties

Nadine Strossen

Follow this and additional works at: https://digitalcommons.nyls.edu/fac_articles_chapters

Part of the [First Amendment Commons](#), [Internet Law Commons](#), and the [Privacy Law Commons](#)

Chapter 8

Cybercrimes vs. Cyberliberties¹

Nadine Strossen

Introduction for the 2009 Edition

I originally wrote my chapter in 1999, when the Internet was a fairly new phenomenon, with which US policymakers and courts were just beginning to grapple. As with all new media, throughout history, too many policymakers and others initially viewed Internet communications as posing unique new dangers to community concerns, including personal safety and national security. Accordingly, government officials reacted to the advent of the Internet in the classic way that government officials have consistently reacted to new media – by restricting freedom of speech and privacy in communications using these new media. The original chapter discusses why such suppressive measures have not even been effective in promoting safety and security, much less necessary to do so.

Elected officials in the USA consistently have supported measures targeting Internet expression, and, true to America's Puritanical heritage, these measures have specifically singled out sexually oriented expression, seeking to shield children from viewing it. In contrast, the courts have consistently struck down such suppressive laws, concluding that the government could more effectively promote its child-protective goals through noncensorial approaches that would also respect adults' rights.

This new Introduction explains how all of the themes and conclusions of the original chapter remain valid despite intervening developments, including the 2001 terrorist attacks. It shows that the major points that the 1999 chapter made about one particular medium, at one particular historical point, concerning particular safety and security issues that were then at the forefront of public concern, apply more universally to other media, during other historical periods, and regarding other safety and security concerns. The Introduction supports this generalization by

N. Strossen
Professor of Law, New York Law School, New York, NY, USA
email: nadine.strossen@nyls.edu

analyzing two sets of subsequent developments. First, it shows that post-911 surveillance measures that target communications, including Internet communications, violate freedom of speech and privacy without sufficient countervailing security benefits. Second, it shows that the government's continuing efforts to suppress online sexual expression, in order to protect children from seeing it, continue appropriately to be struck down by the courts as violating free speech rights without sufficient countervailing benefits.

*Overview: Plus ça Change, Plus c'est la Même Chose*²

Many policy and legal arguments since 2001 have posited a supposedly new post-911 paradigm for many issues, including issues concerning Internet regulation and the (non)protection of free speech and privacy rights in the Internet context.³ However, the allegedly new terrorist dangers, and the allegedly increased justifications for Internet regulations that restrict free speech and privacy in the name of the War on Terror prove, on analysis, to be just the same old.⁴

Before President George W. Bush declared a War on Terror, other US Presidents had declared and maintained a War on Drugs and a War on Crime, invoking strikingly similar rationales. Indeed, even before these metaphorical wars of the past four decades, the USA had been engaged in a cold war, which also raised virtually identical issues about the appropriate balance between government power and individual rights.⁵ The proponents of all of these metaphorical wars have maintained, first, that the USA as a nation, as well as all individuals in the USA, have been facing unprecedented threats to national security, the social order, and/or personal safety. Second, all of these advocates have maintained that, in order to counter the threats in question, government requires increased power, including increased surveillance power over communications, resulting in reduced free speech and privacy rights.

In all of these contexts, though, analysis shows that at least the second part of the common argument is overblown. Thus, even assuming for the sake of argument that the threats posed by terrorism, drugs, and crime are as great as maintained by the proponents of the various wars against them, these warriors still have not satisfied their burden of proving that the increased government powers they advocate actually are necessary to counter the posited threats. Worse yet, many of the new powers are not even effective to counter such threats, let alone necessary. Therefore, they fail to pass muster under the strict scrutiny test that governs measures infringing on fundamental constitutional rights, including free speech and privacy. Under that test, the government must show not only that the rights-restrictive measure is designed to promote a countervailing goal of compelling importance, such as national security or public safety. The government must also show that the challenged measure is narrowly tailored or necessary to promote that goal, and that there is no less restrictive alternative measure, which would also effectively promote the government's goal, with less cost to individual rights.⁶

In the War on Terror, along with other recent metaphorical wars, the increased powers the government has sought to engage in surveillance of Internet and other communications, far from being necessary to advance the government's goals, have to the contrary been criticized by pertinent experts as actually undermining the government's goals. Specifically concerning increased surveillance of Internet and other communications post-9/11, security and counterintelligence experts have maintained that the government's dragnet methods have deflected scarce resources from honing in on the communications of particular individuals regarding whom the government has some basis for suspicion. Moreover, these dragnet methods have deterred many communications that could provide information and insights that could actually aid the government's counterterrorism efforts.⁷

Although I initially wrote the chapter about Cybercrimes and Cyberliberties in 1999, substantially before the 2001 terrorist attacks, and although the US government (as well as governments in other countries⁸) has contended that those attacks warrant extensive new regulations of all communications, including on the Internet, the fundamental points and themes in that chapter remain fully applicable to the post-9/11 world. Both the government arguments in favor of regulation, and the counterarguments in favor of free speech and privacy, have remained essentially the same. The only changes have been the particular factual details that are cited to flesh out what are, at bottom, disagreements about matters of principle: how to strike the appropriate balance between, on the one hand, safety and security, and, on the other hand, liberty and privacy. Indeed, in rereading the 1999 chapter in order to prepare this new Introduction, I was struck by how many of the pertinent factual considerations and policy concerns that the government has stressed in our supposedly new post-9/11 world were also significant before the 2001 terrorist attacks. Even back in 1999, terrorism was of course already a major concern in the USA and many other countries. Accordingly, at the very beginning of the chapter, in its very first line, it recognizes that terrorism, along with crime, is a worldwide concern. Likewise, throughout the chapter, the analysis refers regularly and interchangeably to both crime and terrorism, in assessing competing claims about government regulation and individual freedom. In short, the following is one key takeaway point from the 1999 chapter, which is reinforced by considering the subsequent developments: enduring general themes unify all specific debates about whether restrictions on Internet free speech and privacy are justified for the asserted sake of safety and security.

The themes that I addressed in the 1999 chapter continue to be of general, ongoing relevance in another sense. Although that chapter's specific factual focus was on Internet regulations, it also applies to all communications media beyond the Internet. When I wrote the chapter, the Internet was still quite new in terms of public, political, and press awareness. Accordingly, it generated the same reactions that all new communications media have triggered, throughout history. Proponents of government power, as well as many people who are concerned about safety and security, maintain that the new medium raises unique new risks to these concerns, and therefore warrants unique new regulations. Over the course of the twentieth century, these claims were made successively about the telephone, movies, radio,

broadcast television, cable and satellite television, video cassette recorders, and, most recently, the Internet. The arguments are more alike than different, and indeed parallel the arguments made in support of shutting down that assertedly dangerous new communications innovation introduced by Johannes Gutenberg in the 15th century – the printing press.

Since I am writing this new Introduction to the 1999 chapter almost a decade later, the Internet is no longer so new, and hence, following the historic pattern that has applied to other media, it is no longer regarded as uniquely dangerous. Instead, the Internet is largely considered to be just one of many communications media, all of which raise the same competing concerns regarding safety and liberty, weighing for and against regulations that restrict freedom and privacy of communications. This development, the recognition that the Internet has more in common with other communications media than otherwise, is manifested by the fact that the recent US communications regulations have not singled out the Internet.⁹

Instead, online communications have been included in the same general regulatory initiatives that also have embraced other communications media, and this has specifically been true for post-911 regulations that the government has advocated as countering terrorism, from the US PATRIOT Act¹⁰ in 2001 to the Protect America Act in 2007.¹¹

To sum up what I have said so far, major points that the 1999 chapter made about one particular medium, at one particular historical point, concerning particular safety and security issues that were then at the forefront of public and political consciousness, apply more universally to other media, during other historical periods, and regarding other safety and security concerns. This Introduction will bolster that overarching conclusion by summarizing the most important general points that the 1999 chapter made, and by citing some of the many intervening developments that demonstrate their continuing validity.

The 1999 chapter made two sets of major interrelated points, which have continuing relevance today:

1. Far from being inevitably antagonistic, safety and freedom are often mutually reinforcing. Many measures that are touted as promoting safety are in fact not even effective, let alone necessary, which is the standard that is required by both the US Constitution (as well as the constitutions of many other countries, along with international and regional human rights treaties) and common sense. These generalizations apply to measures that restrict either free speech or privacy online.
2. In addition to protecting safety in general, the US government's other most cited justification for suppressing Internet communications has been to protect children from the alleged adverse effects of exposure to sexually oriented expression, which has traditionally been viewed as especially suspect in American culture and law. Accordingly, it is not surprising that US politicians, of both major political parties, have overwhelmingly voted in favor of laws restricting online sexual expression for the sake of shielding children from it. In contrast, though, US judges have overwhelmingly ruled that these laws are

unconstitutional, and the judges furthermore have stressed that alternative measures, which are less restrictive of free speech and privacy, might well also be more effective in advancing the government's countervailing concerns.

This Introduction will highlight the continued pertinence of these two sets of points by briefly discussing two sets of subsequent developments. First, this Introduction will outline the mutually reinforcing relationship of safety and freedom in the context of government surveillance of communications, including Internet communications, as part of its post-9/11 War on Terror. Second, this Introduction will discuss the judicial rulings that have continued to strike down laws, which politicians continue to support, that suppress online sexual expression for the sake of shielding children.

Post-9/11 Surveillance Measures That Target Communications, Including Internet Communications, Violate Freedom of Speech and Privacy Without Sufficient Countervailing Security Benefits

Ever since the September 11, 2001, terrorist attacks, the ACLU has worked with ideologically diverse allies, including many national security and counterterrorism experts, in what we have called our "Safe and Free" campaign.¹² This name highlights, specifically in the post-9/11 context, the single most important overarching theme of the 1999 chapter: that safety and freedom, far from being inherently antithetical, are often positively interrelated. That theme applies to the government's entire arsenal in its War on Terror, but this Introduction will summarize its pertinence specifically to surveillance measures that target Internet communications, along with other communications.

Starting with the PATRIOT Act, which was enacted just 45 days after the terrorist acts, the US government has exercised increasing surveillance over all communications, including online communications, with measures that violate the fundamental Fourth Amendment¹³ requirements of individualized suspicion and a judicial warrant. Among other things, the PATRIOT Act vastly expanded the government's power to issue National Security Letters (NSLs), demanding that Internet Service Providers (ISPs) turn over information about their customers' online communications, without any judicially issued warrants. The PATRIOT Act also imposed a sweeping gag order on any ISP that receives an NSL, barring the ISP from disclosing any information about this NSL to anyone, including the affected customers.¹⁴ Sweeping and unchecked as these new powers were, we subsequently learned that the Bush Administration had secretly arrogated to itself even more wide-ranging powers to engage in dragnet, suspicionless surveillance of online (and other) communications, without any judicial warrant, using the supersecret National Security Agency (NSA), and also enlisting the telephone companies to turn over their customers' data en masse.¹⁵ The NSA is supposed to be engaged in foreign intelligence gathering against suspected terrorists. However,

as the *New York Times* revealed in December, 2005,¹⁶ ever since 9/11, the NSA been spying on online and phone communications of completely unsuspected (and unsuspecting) American citizens.

In addition to violating the privacy principles that the Fourth Amendment protects, these dragnet communications surveillance measures also violate the freedom of expression principles that the First Amendment¹⁷ protects. Individuals who have reason to fear that their communications will be subject to government spying engage in self-censorship, not using the Internet to discuss or research certain subjects. This chilling effect has especially wide-ranging repercussions when it affects journalists, scholars, and others who seek information to distribute to the public through their research and writings. For example, when their sources will not communicate with them via e-mail, reasonably fearing that the government may be spying on such communications, this violates not only the rights of the would-be parties to these online communications; furthermore, their government-induced self-censorship violates the free speech rights of all potential readers of the suppressed information. As the Supreme Court has stressed, the First Amendment protects the right to receive information and ideas, as well as the right to purvey them.¹⁸ Far from being less important in a time of national security crisis, the right to receive information, including information about government policies, is especially important in such a context, so that We the People,¹⁹ and our elected representatives, can make informed decisions about the especially pressing issues at stake.

Consistent with the foregoing principles, the American Civil Liberties Union ("ACLU") filed a lawsuit challenging the NSA's post-911 warrantless, suspicionless surveillance of Internet and other communications, maintaining that this domestic spying program violates both the Fourth Amendment and the First Amendment. The trial court judge in this case, *ACLU v NSA*, ruled in the ACLU's favor on both constitutional claims.²⁰ The appellate court panel, by a 2–1 vote, dismissed the complaint on technical, jurisdictional grounds, without addressing the merits of the claims.²¹ Notably, the only appellate court judge who did address the merits of the case, having rejected the alleged jurisdictional bars to doing so, agreed with the ACLU and the lower court judge that this sweeping surveillance program was unconstitutional.²²

The ACLU's clients in *ACLU v NSA* included respected, ideologically diverse journalists and scholars who were researching and writing about issues directly related to US counterintelligence policies, including the wars in Afghanistan and Iraq.²³ Therefore, not surprisingly, their sources had particular reasons to desist from online communications, leading to suppression of information that is especially important to everyone in the USA and, indeed, around the world. In short, the government's unwarranted, suspicionless surveillance of online communications through this NSA program was as bad for national security as for individual rights. This point was made as follows by one of the plaintiffs in *ACLU v NSA*, New York University Professor Barnett Rubin, a leading expert on Afghanistan. At the time *ACLU v NSA* was filed, Professor Rubin had been conducting interviews with key individuals in Afghanistan for a report he was doing for the Council on Foreign

Relations, making recommendations for furthering the USA's vital security interests in that strategically significant country.²⁴ As Prof. Rubin said,

[F]or me to provide analysis and updates for the American public and officials who are concerned about Afghanistan, I need to be able to have confidential communications. My experience in Afghanistan convinces me that illegal programs such as warrantless NSA spying... actually undermine national security.²⁵

Along with other constitutional rights and civil liberties, those protected by the Fourth Amendment are fully consistent with promoting national security and public safety. The mutually reinforcing relationship between safety and freedom is illustrated by the fundamental Fourth Amendment principle that is violated by so many post-9/11 programs that involve sweeping surveillance of online communications: The government may not invade anyone's freedom or privacy without individualized suspicion, a particular reason to believe that a particular person poses a threat.²⁶ In short, the Fourth Amendment bars dragnet surveillance measures that sweep in broad groups of people and their communications.²⁷

Of course, the Fourth Amendment's individualized suspicion requirement protects individual liberty. Specifically, it protects each of us from government surveillance of our e-mails and Web surfing based on group stereotyping and guilt by association.²⁸ Moreover, this individualized suspicion requirement also promotes national security. It channels our government's resources – in other words, our precious tax dollars – in the most strategic, effective way toward those persons who actually pose a threat. Precisely for this reason, experts in national security and counterintelligence, as well as civil libertarians, have opposed many of the post-9/11 measures that involve mass surveillance, including mass surveillance of Internet and other communications.²⁹ In short, these measures are the worst of both worlds; they make all of us less free, yet they do not make any of us more safe.

As noted above, one important example of the many doubly flawed post-9/11 mass surveillance measures, which target Internet communications, is the NSA domestic spying program.³⁰ That program has been sweeping in countless e-mails and telephone calls of American citizens who are not suspected of any illegal activity, let alone terrorism.³¹ Therefore, the program's harshest critics include FBI agents.³² The agents complain about the huge amount of time they have been wasting in tracking down the thousands of completely innocent Americans whose electronic communications have been swept up in this NSA fishing expedition.³³

This same dual flaw infects the even more sweeping secret surveillance program, affecting apparently essentially all Internet and telephone communications, which *USA Today* revealed in 2006,³⁴ and which the ACLU is also challenging across the country.³⁵ This massive communications surveillance program apparently³⁶ seeks to collect data about all telephone and online communications from all of the US telephone companies about all of their customers.³⁷ The government asserts that it is using these massive customer calling records for data mining. The government looks for patterns of calls according to certain mathematical formulas that, it says, might point to suspected terrorists.³⁸ However, this whole data-mining approach has been denounced as junk science by prominent experts in mathematics and computer science.³⁹ For example, this perspective was stressed by Jonathan David Farley,

who is not only a mathematics professor at Harvard University, but also a science fellow at Stanford University's Center for International Security and Cooperation.⁴⁰ As he wrote: "[T]he National Security Agency's entire spying program seems to be based on a false assumption: that you can work out who might be a terrorist based on calling patterns. Guilt by association is not just bad law, it's bad mathematics."⁴¹

The NSA domestic spying and data-mining programs, as well as many other post-9/11 surveillance programs, are overly broad dragnets or fishing expeditions. Thus, by definition, they are doubly flawed: they sweep in too much information about too many innocent people, and they make it harder to hone in on the dangerous ones. As one ACLU critic of these surveillance programs memorably put it: "You don't look for a needle in a haystack by adding more hay to the [stack]!"⁴²

The Government's Continuing Efforts to Suppress Sexual Expression, for the Sake of Shielding Children from it, Continue to Be Struck Down by the Courts as Violating Free-Speech Rights Without Sufficient Countervailing Benefits

As the 1999 chapter explained, after the Supreme Court unanimously struck down the first federal law censoring online expression, the Communications Decency Act (CDA),⁴³ in the landmark case of *ACLU v Reno*,⁴⁴ Congress promptly enacted a somewhat narrower law, targeting another category of online sexual expression, which it called the Child Online Protection Act, or COPA.⁴⁵ The ACLU promptly sought and obtained a court order enjoining the government from enforcing this law, on the ground that it violates fundamental free speech principles.⁴⁶ So far, there have been no fewer than seven court rulings on this ACLU challenge to COPA, including two by the US Supreme Court, and all seven rulings have refused to lift the injunction.⁴⁷

The many judges who have ruled in this protracted litigation have espoused a range of reasons for the conclusion that COPA is unconstitutional, including that it is not sufficiently narrowly tailored to promote its goal of shielding children from certain online sexual material that is assumed to be harmful to minors.⁴⁸ In fact, these judges have concluded that COPA is not even effective in shielding minors from the material at issue, and that this goal could be more effectively promoted, instead, by blocking software that individual parents install on their own children's computers. Of course, such user-based blocking software, which is utilized only by particular individuals who opt to do so, is completely consistent with First Amendment principles. Therefore, in this context, as well as the post-911 context, the chapter's overarching conclusion is once again reaffirmed; protecting civil liberties online is fully consistent with government's countervailing concerns, far from being antithetical to them.

The second time the Supreme Court ruled on COPA, in 2004, the Court recognized that user-based blocking software was likely more effective than COPA's criminal bar as a means of restricting childrens' access to materials harmful to them.⁴⁹ Because the trial in the COPA case had taken place in 1999, the Supreme Court's 2004 ruling remanded the case to the trial court to reconsider that conclusion, in light of intervening technological developments. The second trial, on that remand, took place in the fall of 2006. Based on the extensive, updated evidentiary materials presented at that second trial, following the Supreme Court's remand, the trial court once again concluded that the government had failed to show that COPA is the least restrictive alternative for advancing Congress's interest in protecting minors from exposure to sexually explicit material on the World Wide Web.⁵⁰ Moreover, the court concluded that the government "failed to show that other alternatives are not at least as effective as COPA."⁵¹ To the contrary, the court concluded that user-based blocking or filtering programs are actually more effective than COPA, for several reasons, including the following: filters block sexually explicit online material that is posted outside the USA, and individual parents can customize the settings of filters according to the ages of their children and what type of content those parents find objectionable.⁵²

In sum, the courts that have ruled on COPA have repeatedly concluded that children's online safety, as well as adults' online free speech, are more effectively promoted not through censorship, but rather through alternative measures that enhance freedom of choice for all adults and parents. This same conclusion has also been reached by both of the two expert government commissions that have recently examined how best to shield children from online sexual material that their parents might deem inappropriate for them. One panel was authorized by Congress in the COPA statute itself,⁵³ and the other panel was convened by the prestigious National Research Council (NRC).⁵⁴ Both groups were very diverse, including leading antipornography activists as well as Internet experts.⁵⁵ The NRC panel was chaired by Richard Thornburgh, a conservative Republican who had served as US Attorney General under Presidents Reagan and Bush I. All members of both commissions rejected the proposition that online sexual material should be regulated to prevent minors from accessing it. Instead, both groups most strongly recommended social and educational strategies that teach children to make wise choices about using the Internet.⁵⁶ Of course, that alternative is completely consistent with free speech rights, including the free speech rights of children themselves,⁵⁷ as well as those of adults.

In addition to the two post-1999 Supreme Court decisions sustaining the ACLU's constitutional challenge to COPA, the Court has issued one other post-1999 decision ruling on one other federal law that suppresses certain Internet expression – the Children's Internet Protection Act (CIPA).⁵⁸ Consistent with the pattern that the 1999 chapter describes, this law, along with the CDA and COPA, singles out online sexual expression in particular, and also focuses on harms that are assumed to be caused to children in particular as a result of viewing such expression.⁵⁹ Again following the pattern that the 1999 chapter outlined, the courts

that ruled on CIPA, including the Supreme Court, have continued consistently to limit government power to restrict adults' online free speech rights for the purported sake of shielding minors from exposure to online sexual expression.

In 2003, in *United States v American Library Association*,⁶⁰ the Supreme Court narrowly construed CIPA in order to restrict its interference with adults' online free speech and privacy rights. CIPA requires all public libraries that receive certain government funding, as a condition of that funding, to install blocking software on all library computer terminals, which is designed to block certain sexually oriented material. In a fragmented ruling, with no majority opinion, six Justices in total, for various reasons, rejected a facial challenge that the ACLU and the American Library Association (ALA) had brought to CIPA; in other words, the ACLU and the ALA sought to invalidate CIPA altogether, no matter how it was enforced. However, these six Justices rejected the facial challenge only after construing CIPA very narrowly, in a way that respected the free speech and privacy rights of adults who access the Internet at affected public libraries.

Specifically, in their three separate opinions, all of these Justices stressed that any time an adult library patron asked to have the blocking software turned off, the library staff had to do so automatically and promptly, without seeking any information from any such adult.⁶¹ Moreover, a majority of the Justices stressed that if CIPA were ever enforced in a way that did infringe on the free speech or privacy rights of adult library patrons, then CIPA would be vulnerable to a constitutional challenge on an as-applied basis, invalidating any such enforcement.⁶²

In fact, in 2006, the ACLU instituted an as-applied challenge to CIPA as it was enforced by certain libraries in Washington state, which did block adult patrons' access to various Internet sites, including sites that had no sexual content.⁶³

Conclusion

Although I initially wrote my chapter in 1999, before the 2001 terrorist attacks, all of its themes and conclusions retain their force. Analysis of the post-911 measures for government surveillance of Internet communications reinforces the conclusion that we need not sacrifice online privacy and free speech in order to promote personal safety or national security. Likewise, the same general conclusion, that safety and freedom are compatible concerns, is also reinforced by the post-1999 judicial rulings about US statutes that suppress online sexual expression in order to protect children from seeing it. These rulings further reaffirm that measures suppressing Internet free speech and privacy are the worst of both worlds; they do curtail individual liberty, but they do not effectively advance countervailing safety or security goals.

The Thomas Jefferson insight that I quoted in the 1999 chapter remains enduringly prescient today, two centuries after he uttered it: "A society that will trade a little liberty for a little order will deserve neither and will lose both."⁶⁴

Original Chapter: Introduction

Cyberspace is an inherently global medium. Cybercrime and terrorism are world-wide concerns. Preserving human rights in cyberspace is also an international concern.

This chapter reviews legal developments in the USA, which has had more legislation and litigation in this area than has any other country. Our courts' rulings, of course, have been grounded on US law – in particular, the free-speech guarantee of the First Amendment to our Constitution and our constitutional right of privacy. Those same freedoms, however, 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.⁶⁵ Therefore, the principles that have guided legal developments in the USA should be relevant in the British Isles and elsewhere, just as developments in Britain and in other parts of the world are relevant in the USA.

Overview of Interrelationship Between Cybercrime and Cyberliberties

The interrelationship between cybercrime and cyberliberties is a broad subject that encompasses two major subtopics. The first subtopic is 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. The second subtopic is 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; the second subtopic 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 individual rights and public safety. In fact, though, this alleged tension is oversimplified and misleading. In terms of advancing public safety, measures that stifle cyberliberties are often ineffective at best and counterproductive at worst. 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: “A society that will trade a little liberty for a little order will deserve neither and will lose both.”⁶⁶ This statement is right on the mark, for several reasons, concerning the current debates about cybercrimes and cyberliberties. First, claims about the allegedly 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 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, director of the National Center for Missing & Exploited Children in the USA, 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 allegedly are harmful to children's minds is a dangerous distraction and diversion from constructive efforts to protect actual children from tangible harm.⁶⁷

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. I say "everyone" advisedly, as young people have free speech rights of their own.⁶⁸

The same false tension between liberty and security also makes 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 be aided to some extent if officials could gain access easily 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.⁶⁹ The consensus of the international community is that this violation 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?⁷⁰

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 Court⁷¹:

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.⁷²

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 who will not comply with government restrictions on encryption. To the contrary, criminals and terrorists will take all available measures, including illegal measures, to secure their own communications. Meanwhile, thanks to legal limits on encryption, cybercriminals will prey more easily 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 cyberlibertarians in opposing limits on encryption. They concur that, on balance, such limits do more harm than good to public safety.⁷³

In broad overview, the relationship between cyberliberties and crime control is not inherently antagonistic but, rather, is often mutually reinforcing. In many respects, law and public policy are developing in a way that is consistent with this perspective. US courts consistently have struck down new laws that seek to criminalize expression online that would be legal in other media. Many judges who have ruled on such laws have agreed with the American Civil Liberties Union (ACLU) and other cyberlibertarians that the laws are not well designed for protecting children, which is their asserted goal. These judges include the entire US Supreme Court, ruling in the landmark 1997 case that struck down the first federal Internet censorship law in the USA, the CDA,⁷⁴ in *Reno v ACLU*.⁷⁵

Now we have to call that case *ACLU v Reno I*, since the US federal government subsequently enacted its second cybercensorship law, the so-called Child Online Protection Act or COPA,⁷⁶ which at the time of this writing is being fought in a case called *ACLU v Reno II*.⁷⁷ It is not surprising that few politicians had the political courage to oppose a law with a name like the "Child Online Protection Act." Fortunately, though, the only judge to rule on the law to date has agreed with us that it not only is unconstitutional but also is unwise and misnamed, as it does not really protect children. Indeed, he concluded his opinion on this note:

Perhaps 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.⁷⁸

When we turn from online free speech to privacy, the US courts have been likewise 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*,⁷⁹ we successfully challenged a state law that prohibited anonymous and pseudonymous online communications. There have, though, been fewer rulings concerning privacy than concerning free speech in the online context. Rulings concerning privacy have been issued only by lower-level courts, and they have not been as consistently supportive of the cyberliberties positions.⁸⁰

In the USA, the battle over online privacy and encryption is being waged mostly in the legislative and executive branches of government, rather than in the courts. The Clinton Administration steadily opposed strong encryption, but many members of Congress, from both major political parties, were on the other side.

Thus far, at least, the US government is quite isolated in the international community in this respect, as most other countries allow strong encryption.⁸¹ There is certainly a preference for strong encryption in Europe, which in general has stronger legal protections for privacy of communications and data than we have in the USA.⁸² The Clinton Administration, however, worked hard to export its antiprivacy, antientryption stance around the world,⁸³ and it did gain support from some officials in Britain. It is essential, therefore, to understand why this stance is as inimical to public safety as it is to personal privacy.

Criminalizing Sexually Oriented Online Expression

With this general picture of the relationship between cyberliberties and cybercrime, let us next fill in some details, starting with the area where we have had the most legislation and litigation in the USA. This is also an area of great concern in other countries, namely, criminalizing online expression that is sexually oriented.⁸⁴

From the moment that cyberspace first hit the public radar screen in the USA, 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, sexually oriented expression in any medium has been suspect throughout our history. That is because of our Puritanical heritage, which we share, of course, 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.⁸⁵

Consistent with this long-standing American tradition, we have seen many efforts throughout the USA to stifle online sexual expression. This has transpired at all levels of government, from the US Congress and the Clinton Administration to local school boards and library boards.⁸⁶ From a free-speech perspective, that is the bad news about sexually oriented expression online. But there is good news, too. While elected officials mostly have supported censorship of sexually oriented online material, the courts, as I have indicated, have provided a welcome contrast. So far, the ACLU has brought constitutional challenges to seven new laws that censor sexually oriented material online: the two federal statutes I already mentioned,⁸⁷ four state laws (in New York,⁸⁸ Virginia,⁸⁹ New Mexico,⁹⁰ and Michigan⁹¹), and one local law (in Loudoun County, Virginia⁹²). And so far, with only one recent exception – which I do not think is too significant for cyberliberties, as I will explain in a moment – we have won every single one of these challenges.

Moreover, these decisions affirming freedom of cyberspeech have been joined in by 19 different judges who span a broad ideological spectrum. These are judges who were appointed by the last six US Presidents, four Republicans, and two Democrats, going all the way back to Richard Nixon. 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 that restricts government employees’ access to sexually oriented online material.⁹³ 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.⁹⁴ Nevertheless, the lower court agreed with us that Virginia’s law violates even the reduced free-speech rights of government employees.⁹⁵ The intermediate appellate court subsequently overturned that decision in February, 1999, on the broad rationale that government employees, when they act primarily in their role as employees,

have no free-speech rights concerning any communications in any medium.⁹⁶ This court maintained that it 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 is wrong, and we hope to overturn it on further appeal. In any event, though, it really has no special impact specifically on cyberlaw or cyberliberties.

In contrast, our two most recent victories in cybersensorship cases do have broad positive implications for online free speech, and I would like to describe them. 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 cybersensorship law, COPA. In response to the Supreme Court's decision striking down the CDA in *ACLU I*,⁹⁷ Congress wrote a somewhat less sweeping law the second time around. The CDA had criminalized any online expression that is "patently offensive"⁹⁸ or "indecent."⁹⁹ In contrast, the Child Online Protection Act (COPA) outlaws any online communication "for commercial purposes"¹⁰⁰ that includes any material that is harmful to minors.¹⁰¹

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.¹⁰² Therefore, COPA applies to many not-for-profit Web sites that provide information completely free, including the ACLU's own Web site. Second, material is "harmful to minors" if it satisfies US law's three-part obscenity definition specifically with respect to minors, namely, if it appeals to the prurient interest in sex, is patently offensive, and lacks serious value from a minor's perspective.¹⁰³

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).¹⁰⁴ However, we have not used our cybersensorship 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 that 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 are unprotected specifically online, even though it would be constitutionally protected in traditional print media.

With that perspective, let me turn back to *ACLU v Reno II*. On February 1, 1999, a federal judge, Lowell Reed, granted our motion for a preliminary injunction.¹⁰⁵ 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,"¹⁰⁶ 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 that would be less burdensome on free speech.¹⁰⁷

Judge Reed concluded that the government does have a compelling interest in shielding minors even from materials that are not obscene by adult standards.¹⁰⁸ However, he also concluded that the government was unlikely to be able to show that COPA is the least restrictive means of achieving this goal.¹⁰⁹ He noted, for example, 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.”¹¹⁰ The government has appealed from Judge Reed’s ruling.¹¹¹ Quite likely, this case will go all the way to the US Supreme Court that has issued only one decision on the “harmful to minors” doctrine, and that was more than 30 years ago.¹¹²

Now let me turn to a second victory, in another important cyberspeech case, which also is still working its way through the court system at the time of this writing. This case is called *Mainstream Loudoun v Loudoun County Library*,¹¹³ 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 are facing constitutional difficulties, advocates of suppressing online sexual expression stepped up their promotion of rating and filtering systems, which also would bar access to the same expression. The ACLU has issued two reports explaining many reasons why all these systems are problematic.¹¹⁴ For one thing – in terms of blocking all the material it purports to, and only that material – the filtering software is inevitably both underinclusive and overinclusive. 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. Manufacturers 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.

There is a serious free-speech problem, however, when the filtering software is installed not as a matter of choice by individual users but, rather, by government officials who control the computers in public institutions. Across the USA, officials are busily installing or advocating blocking software on computers in public libraries, schools, and universities.¹¹⁵ Individual choice thereby 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.

Book banning, in fact, 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 public libraries of Loudoun County, Virginia.¹¹⁶ Pursuant to a “Policy on Internet Sexual Harassment,” library officials required software to block “child pornography and obscene material,” as well as material deemed “harmful to juveniles” under state law.¹¹⁷

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.¹¹⁸

Even beyond their misguided concept of sexual harassment, library officials also implemented their 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 also has been applied to other censorial laws, such as CDA and COPA.¹¹⁹

Judge Brinkema assumed for the sake of argument that the government's asserted interests – namely, its interests in minimizing access to obscenity and child pornography and in avoiding the creation of a sexually hostile environment – were of compelling importance.¹²⁰ She concluded, however, 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."¹²¹

One particularly interesting feature of Judge Brinkema's analysis is her catalog 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, and 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.¹²² 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.¹²³ Loudoun County officials decided not to appeal from Judge Brinkema's ruling.¹²⁴ Of course, the constitutional questions involved will not be settled until the US Supreme Court rules on them in another filtering controversy.¹²⁵

Debates About Online Privacy and Cryptography

This section discusses further the second major aspect of the cyberliberties/cyber-crime debate – 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 debunked effectively by Brian Gladman in "Cyber-Crime and Information Terrorism," an excellent report that was issued in September, 1998:

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.¹²⁶

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 use, precisely because they did fear that it would facilitate criminal activities.¹²⁷ Today that argument seems ludicrous but, at bottom, it is precisely the same as the one now being offered in an attempt to justify restrictions on cryptography.

This is the argument the Clinton Administration made. They insisted 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, as 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, that in fact is not so. To the contrary, this situation vividly illustrates Thomas Jefferson's previously quoted observation: "Liberty and security concerns work in tandem, rather than in tension, with each other. Indeed, it is particularly apt, in the cryptography context, to refer to Jefferson's communications with Madison; when these two American founders corresponded prior to the signing of the Declaration of Independence, they encoded all their messages. They used eighteenth-century-style encryption!"¹²⁸

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 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 USA.¹²⁹

Accordingly, even though this NRC report recognized that restricting encryption would strengthen some law enforcement efforts, it nevertheless concluded the following:

On balance, the advantages of more widespread use of cryptography outweigh the disadvantages.¹³⁰

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 the USA has enforced and advocated, that is, 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.¹³¹

For these 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 issue of the 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.¹³² He dismissed government and media descriptions of the dangers of cyberterrorism as “myths,”¹³³ “hoaxes,”¹³⁴ and “the electronic ghost stories of our time.”¹³⁵ Although the Smith study focused on the USA, it is no doubt relevant for other countries also. Here is its conclusion:

The government’s evidence about US 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 thus far provided.... casts a great deal of doubt on the claims.¹³⁶

Precisely the same conclusion was reached in a report by a commission appointed by President Clinton on “Critical Infrastructure Protection.”¹³⁷ The Commission was charged with analyzing the danger that information terrorists could pose to our nation’s infrastructure – communications lines, power grids, and transportation networks. The Commission consisted primarily of military and intelligence officials and therefore was presumed to be especially sympathetic toward government claims of threats to law enforcement and national security. 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.”¹³⁸

Nonetheless, that recognition did not deter the Commission from seizing upon the fear of cyberterrorism to press for government measures – including key recovery encryption – that constrict individual rights. Indeed, the Commission was so eager to leverage public concerns about infoterrorism 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!¹³⁹ Brian Gladman described those dangers well in “Cyber-Crime and Information Terrorism,” the report from which I quoted earlier:

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 organisations using only modest resources. Cryptographic export 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.¹⁴⁰

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

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.¹⁴¹

In sum, not only are claims about the dangers of cyberterrorism exaggerated but also the proposed countermeasures – 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 government reports present precisely the same conclusions. In September, 1999, for example, a European Parliament report called for rejecting encryption controls, including those advocated by the USA.¹⁴² 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.¹⁴³ This pattern was documented by a comprehensive report that GILC issued in February, 1998, entitled *Cryptography and Liberty 1998*. This report 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:

For those [countries] that have considered the topics, interests in electronic commerce and privacy appear to outweigh the concerns expressed by law enforcement.¹⁴⁴

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.¹⁴⁵

Notes

1. This new introduction was completed in May, 2008. For assistance with research and endnotes, the author gratefully acknowledges her Chief Aide, Steven Cunningham (NYLS '99), who bears both credit and responsibility for the endnotes. Valuable research assistance was also provided by Graig Craver (NYLS '09).
2. The more things change, the more they stay the same.
3. See, for example, Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency (Inalienable Rights)* (New York: Oxford University Press, 2006).
4. See, for example, James Cole and Jules Lobel, *Less Safe, Less Free: Why America Is Losing the War on Terror* (New York: New Press, 2007).
5. See, for example, "A Bill to Repeal Certain Cold War Legislation and for Other Purposes," S. 236, introduced January 17, 1991 (102nd Congress) by Senator Daniel Patrick Moynihan (D-NY).
6. Erwin Chemerinsky, *Constitutional Law: Principles and Policies*, 694–695 (New York: Aspen, 3rd edn., 2006).
7. Richard A. Clarke, "Bush Legacy: Setting a Standard in Fear-Mongering," *Philadelphia Inquirer*, February 8, 2008; Bruce Schneier, *Beyond Fear* (New York: Springer Press, 2004).
8. See, for example, "Application No. 2947/06: Ismoilov and Others v. Russia Intervention," Submitted by Human Rights Watch and AIRE Centre (New York: Human Rights Watch, 2007); "UK: Counter the Threat or Counterproductive?" Commentary on Proposed Counterterrorism Measures (New York: Human Rights Watch, 2007); Judith Sunderland, "In the Name of Prevention Insufficient Safeguards in National Security Removals" (New York: Human Rights Watch, 2007) (France); Joanne Mariner, "Double Jeopardy CIA: Renditions to Jordan" (New York: Human Rights Watch, 2008); Joanne Mariner, "Ghost Prisoner: Two Years in Secret CIA Detention" (New York: Human Rights Watch, 2007) (Israel), *all available at*: http://www.hrw.org/doc/?t'ct_pub

9. This Introduction discusses only nationwide regulations, enacted by the US government. Accordingly, the statement in this sentence applies only to such regulations. In contrast, at the state level, some recent regulations have specifically singled out the Internet. It should be noted, though, that courts have struck down many such state regulations on various constitutional and statutory grounds, including on the ground that the US Constitution and/or US statutes preempt state regulation. *See*, for example, H. Russell Frisby, Jr. and David A. Irwin, "The First Great Telecom Debate of the 21st Century," 15 *CommLaw Conspectus* 373 (2007); Transcript: "The Federalist Society Presents its 2006 Telecommunications Federalism Conference: Intro and Opening Remarks," *B.C. Intell. Prop. & Tech. F.* 165 (2007); *Ctr. for Democracy and Tech. v. Pappert*, 337 F. Supp. 2d 606 (E.D. Pa. 2004) (striking down Pennsylvania Internet censorship law as inconsistent with the First Amendment and Dormant Commerce Clause); 47 U.S.C. §230 (preempting state laws imposing liability on Internet intermediaries for material supplied by users); *Voicenet Commun. Inc. v. Corbett*, No. 04-1318, 2006 US Dist LEXIS 61916 (E.D. Pa. 2006) (applying §230 to preempt application of state anti-pornography law to Internet service provider).
10. Pub. Law No. 107-56, 115 Stat 272; Title I-§105; Title II-§§201, 202, 204, 209, 210, 211, 212, 214, 215, 216, 217, 220, 225 Title VIII §814, Title X §1003 (October 26, 2001) *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*.
11. Pub.L. No. 110-055_1, 121 Stat 552, enacted 50 U.S.C. §1805(a)-(c) amended 50 U.S.C. §1803 (August 5, 2007) *Clarification of Electronic Surveillance of Persons Outside the United States*.
12. Nadine Strossen, Safety and Freedom: Common Concerns for Conservatives, Libertarians, and Civil Libertarians, 29 *Harv. J.L. & Pub. Pol'y* 73 (2005); ACLU Safe and Free Campaign website: <http://www.aclu.org/safe/free/index.htm>
13. US CONST, AMEND. IV (The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized).
14. Pub.L. No. 107-56, 115 Stat. 272 (October 26, 2001) *USA PATRIOT Act*, NSL parts codified in 18 U.S.C. §§2709, 2709 was originally enacted as part of Title II of the Electronic Communication Privacy Act of 1986, Pub.L. No. 99-508, '201, 100 Stat. 1848, 1867-1868 (1986). Congress then passed the US Patriot Improvement and Reauthorization Act of 2005, Pub.L. No. 109-177, 120 Stat. 192 (March 9, 2006). The Reauthorization Act included substantial changes to §2709 and added several provisions relating to judicial review of NSLs which were codified in 18 U.S.C. a 3511 Congress made further changes to §2709 in the US Patriot Act Additional Reauthorizing Amendments Act of 2006, Pub.L. No. 109-178, 120 Stat. 278 (March 9, 2006). This act amended §2709(c)(4), which requires NSL recipients to inform the FBI of anyone to whom they disclosed having received the NSL, with the exception of counsel, and it added §2709(f), which excludes libraries from the definition of wire or electronic communications service providers. *Doe v. Gonzalez*, 500 F. Supp. 2d 379, 384-387.
15. Leslie Cauley, "NSA has massive database of Americans' phone calls," *USA Today*, May 11, 2006; John Markoff, "Questions Raised for Phone Giants in Spy Data Furor," *New York Times*, May 13, 2006.
16. James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," *New York Times*, December 16, 2005.
17. US CONST, AMEND. I (Congress shall make no law ... abridging the freedom of speech, or of the press...).
18. *Stanley v. Georgia*, 394 US 557, 564 (1969).
19. US CONST, PREAMBLE (We the People of the United States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America).

20. *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *stay granted*, 467 F.3d 590 (6th Cir. 2006), *vacated and remanded*, 493 F.3d 644 (6th Cir. 2007), *cert. denied*, 128 S. Ct. 1334 (2008).
21. *ACLU v. NSA*, 493 F.3d 644.
22. *ACLU v. NSA*, 493 F.3d at 693 (Gilman, dissenting).
23. *ACLU v. NSA* Complaint filed January 17, 2006 in US District Court for the Eastern District of Michigan, Southern Division at pages 2, 44, 46, 4, 50. Available at: <http://www.aclu.org/pdfs/safe/free/nsacomplaint.011706.pdf>
24. Barnett A. Rubin, *Afghanistan's Uncertain Transition from Turmoil to Normalcy* (New York: Council on Foreign Relations Press, April 2006).
25. ACLU Press Release, "Federal Court Strikes Down NSA Warrantless Surveillance Program," August 17, 2006. Available at: www.aclu.org/safeandfree/nsaspying/26489prs20060817.html (last accessed May 15, 2008).
26. See US CONST, AMEND. IV; *Michigan Dept. of State Police v. Sitz*, 496 US 444, 449–450 (1990).
27. See, for example, *Davis v. Mississippi*, 394 US 721, 723–725 (1969) (suspects were wrongfully detained by police merely because of the color of their skin).
28. *Ibid.*, 726.
29. See, for example, ACLU Press Release, "Applauds Local Police Departments for Refusing to Join in Justice Department Dragnet" (March 4, 2002), available at: <http://www.aclu.org/police/gen/14530res20020304.html>
30. See, for example, *ACLU v. NSA*, 438 F. Supp. 2d 754.
31. See, for example, *ACLU v. NSA*, 438 F. Supp. 2d at 773–775.
32. See, for example, Lowell Bergman et al., "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," *New York Times*, January 17, 2006.
33. *Ibid.* (FBI officials repeatedly complained to the spy agency that the unfiltered information was swamping investigators and said that the torrent of tips led them to few potential terrorists inside the country they did not know of from other sources and diverted agents from counter-terrorism work they viewed as more productive.)
34. Leslie Cauley, "NSA Has Massive Database of Americans' Phone Calls," *USA Today*, May 11, 2006.
35. See generally *ACLU v. NSA*, 438 F. Supp. 2d at 754; *Doe v. Gonzales*, 386 F. Supp. 2d 66 (D. Conn. 2005); ACLU, Safe and Free: Secrecy, available at: <http://www.aclu.org/safe/free/secrecy/index.html>
36. I include the qualifying word "apparently" since the clandestine nature of this program as well as conflicting government statements about it in the wake of the USA Today disclosure have obscured its precise nature. See "A Note to Our Readers," *USA Today*, June 30, 2006; Frank Ahrens and Howard Kurtz, "USA Today Says It Can't Prove Key Points in Phone Records Story," *Star-Ledger* (Newark, New Jersey), July 2, 2006.
37. Cauley, *supra* note 34.
38. See, for example, *Elec. Privacy Info. Ctr. v. Dep't of Def.*, 355 F. Supp. 2d 98, 99 (D.D.C. 2004).
39. See Computer Professionals for Social Responsibility Press Release, "CPSR Signs ACLU Letter Supporting 132," October 23, 2005, available at: <http://www.cpsr.org/issues/privacy/support132>; see also Jonathan David Farley, "The N.S.A.'s Math Problem," *New York Times*, May 16, 2006.
40. *Ibid.*
41. *Ibid.*
42. Barry Steinhardt, ACLU Press Release, "Statement of Barry Steinhardt, Director Technology and Civil Liberty Program, American Civil Liberties Union, On Government Data Mining, Before the: Technology, Information Policy, Intergovernmental Subcommittee of the House of Representatives Committee on Government Reform" on May 20, 2003. Available at: <http://www.aclu.org/safe/free/general/17262leg20030520.html>
43. 47 U.S.C. §223 (1996).

44. 521 US 844 (1997).
45. 47 U.S.C. §231 (1998).
46. *ACLU v. Reno*, 31 F. Supp. 2d 473 (E.D.Pa. 1999).
47. These rulings, listed in chronological order, are: *ACLU v. Gonzales*, 478 F. Supp. 2d 775 (E.D.Pa. 2007); *Ashcroft v. ACLU*, 542 US 656 (2004); *ACLU v. Ashcroft*, 322 F.3d 240 (3rd Cir. 2003); *Ashcroft v. ACLU*, 535 US 564 (2002); *ACLU v. Reno*, 217 F.3d 162 (3rd Cir. 2000); *ACLU v. Reno*, 31 F. Supp. 2d 473 (E.D.Pa. 1999); *ACLU v. Reno*, 1998 WL 813423 (E.D.Pa. 1998).
48. See, for example, *ACLU v. Ashcroft*, 322 F.3d 240 (3rd Cir. 2003); *ACLU v. Gonzales*, 478 F. Supp. 2d 775 (E.D.Pa. 2007); *ACLU v. Reno*, 31 F. Supp. 2d 473 (E.D.Pa. 1999).
49. *Ashcroft v. ACLU*, 542 US 656, 667 (2004).
50. *ACLU v. Gonzales*, 478 F. Supp. 2d 775, 813–814 (E.D. Pa. 2007).
51. *Ibid*, 814–816.
52. *Ibid*, 814–815.
53. 47 U.S.C. §231 (2000) (Established Commission on Online Child Protection).
54. Dick Thornburgh and Herbert S. Lin, eds. *National Resource Council, Youth Pornography, and the Internet* (New York: National Academy Press, 2002).
55. John Schwartz, “Support is Growing in Congress for Internet Filters in Schools,” *New York Times*, October 20, 2000.
56. National Research Council Press Release: “Youth Pornography, and the Internet.” Available at: <http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID%2061>
57. The Supreme Court has repeatedly held that minors, as well as adults, have free speech rights. See, for example, *Tinker v. Des Moines Ind. Comm. School Dist.*, 393 US 503 (1969).
58. 47 U.S.C. §254 (2000).
59. Since 1999, the Supreme Court also has issued two decisions that I will briefly note here, but not discuss in the text, since they address two US statutes that are only indirectly relevant to the issues considered in this new Introduction and the 1999 chapter. These two cases are: *U.S. v. Williams* 2008 WL 2078503 (2008) [Concerning the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act, 18 U.S.C. ‘2252(A)(a)(3)(b)] and *Free Speech Coalition v. Ashcroft* 535 US 234 (2002) [concerning the Child Pornography Prevention Act, 18 U.S.C. §§2256(8)(A), 2256(8)(B), 2256 (8)(C), 2256 (8)(D)]. Both cases are beyond the scope of this Introduction for two reasons. First, the laws at issue did not single out the Internet, but rather, targeted all expression with the prohibited content, in any medium. Second, these laws did no seek to protect children from viewing sexually oriented expression, but rather, they sought to protect children from being used to produce child pornography. It should be noted, however, that both statutes, as well as both Supreme Court decisions, protected adults’ rights to view even virtual child pornography, sexually explicit images that look like child pornography, but that are produced without using actual minors. In that significant respect, both cases are consistent with the general speech-protective pattern of the judicial rulings that the 1999 chapter and the new Introduction discuss.
60. 539 US 194 (2003).
61. 539 US 194, 209 (plurality opinion), 214 (Kennedy, J., concurring), 220 (Breyer, J., concurring).
62. *Ibid*, 215 (Kennedy, J., concurring), 220 (Breyer, J., concurring), 233 (Souter, J., dissenting).
63. As of May, 2008, this lawsuit was still pending, with no ruling yet on the merits. See *Bradburn v. North Central Regional Library District* Complaint filed November 16, 2006 in US District Court Eastern District of Washington. Both available at: <http://www.aclu-wa.org/detail.cfm?id%20557>; ACLU Press Release, *ACLU Suit Seeks Access to Information on Internet for Library Patrons* (November 16, 2006, updated April 23, 2008).
64. *Williams v. Garrett*, 722 F. Supp. 254, 256 (W.D. Va. 1989) (quoting Thomas Jefferson).
65. See, for example, Global Internet Liberty Campaign, *Regardless of Frontiers: Protecting the Human Right to Freedom of Expression on the Global Internet*, 1998; Global Internet Liberty Campaign, *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*, 1998.

66. *Williams v. Garrett*, 722 F. Supp. 254, 256 (W.D. Va. 1989) (quoting Thomas Jefferson).
67. See Nadine Strossen and Ernie Allen, "Megan's Law and the Protection of the Child in the Online Age," *American Criminal Law Review*, 35, no. 4 (summer 1998): 1319-1341. 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." (See Nadine Strossen, "Bang the Tin Drum No More," *Speakout.com*, July 17, 1997 <http://www.speakout.com/activism/opinions/3669-1.html>.)
68. See *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 212 (1975) ([M]inors are entitled to a significant measure of First Amendment protection.); *Tinker v. Des Moines Indep. Community Sch. Dist.*, 393 U.S. 503, 506 (1969) (First Amendment rights... are available to... students...); United Nations Children's Fund (1989) *Convention on the Rights of the Child*. See Article 13 under "Convention Full Text" tab from <http://www.unicef.org/crc/crc.htm>: "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."
69. See Electronic Privacy Information Center, *Cryptography and Liberty 1999: An International Survey of Encryption Policy* (1999), <http://www2.epic.org/reports/crypto1999.html>, 8.
70. 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.
71. See S.D. Warren and L.D. Brandeis, "The Right to Privacy," *Harvard Law Review*, 4 (1890) 193.
72. See *Olmstead v. United States*, 277 U.S. 438, 485 (1928) (Brandeis, J. dissenting), overruled by *Katz v. United States*, 389 U.S. 347 (1967).
73. See National Research Council, *Cryptography's Role in Securing the Information Society*, eds. Kenneth W. Dam and Herbert S. Lin (Washington, DC: National Academy Press, 1996), <http://www.nap.edu/readingroom/books/crisis/>.
74. See 47 U.S.C. Section 223 (a, d) (1999).
75. See *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
76. See 47 U.S.C. Section 231 (1999).
77. See *American Civil Liberties Union v. Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999).
78. *Id.*, at 498.
79. See *American Civil Liberties Union v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997).
80. *Bernstein v. U.S.*, 974 F. Supp. 1288 (N.D. Ca. 1997), *aff'd*, 176 F. Supp. 3d 1132 (9th Cir. May 6, 1999) (holding that encryption regulations were an unconstitutional prior restraint in violation of the First Amendment). But cf. *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 Dept. 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. See J. Clausing, "In a Reversal, White House Will End Data-Encryption Export Curbs," *New York Times*, September 17, 1999. 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; see Electronic Frontier Foundation, "Latest Governmental Encryption Scheme Still Unconstitutional: EFF-Sponsored Legal Challenge Will Proceed," September 16, 1999, http://www.eff.org/91699_crypto_release.html. In 1999, the Ninth Circuit withdrew the three-judge panel decision in *Bernstein* and ordered the case to be reheard *en banc*. *Bernstein v. U.S.*, No. 97-16686, 1999 US App. LEXIS 24324 (9th Cir. September 30, 1999).

81. See Global Internet Liberty Campaign, Wayne Madsen et al., "Cryptography and Liberty 1998: An International Survey of Encryption Policy," February 1998. <http://www.gilc.org/crypto/crypto-survey.html>, 5.
82. *Ibid.*
83. *Ibid.*, 6.
84. See Y. Akdeniz and N. Strossen, "Obscene and Indecent Speech," in *The Internet, Law and Society*, eds. C. Walker, Y. Akdeniz, and D. Wall (Essex: Addison Wesley Longman, 2000).
85. See Garrison Keillor, Statement to the Senate Subcommittee on Education, March 29, 1990 (Testimony on NEA Grant Funding and Restrictions) 136 Cong. Rec. E. 993 (1990).
86. See American Civil Liberties Union Freedom Network, "Cyber-Liberties," <http://www.aclu.org/issues/cyber/hmcl.html>.
87. See *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).
88. See *American Library Assn v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997).
89. See *Urofsky v. Allen*, 995 F. Supp. 634 (E.D. Va. 1998), overruled by *Urofsky v. Gilmore*, 167 F. 3d 191 (4th Cir. 1999).
90. See *American Civil Liberties Union v. Johnson*, 4 F. Supp. 2d 1029 (D.N.M. 1998).
91. See *Cyberspace v. Engler*, 55 F. Supp. 2d 737 (E.D. Mich. 1999).
92. See *Mainstream Loudoun v. Loudoun County Library*, 24 F. Supp. 2d 552 (E.D. Va. 1998).
93. See *Urofsky v. Gilmore*, 167 F. 3d 191 (4th Cir. 1999).
94. See *Waters v. Churchill*, 511 U.S. 661, 674–675 (1994); *Pickery v. Board of Educ.*, 391 U.S. 563, 568 (1968).
95. See *Urofsky v. Allen*, 995 F. Supp. 634 (E.D. Va. 1998).
96. See *Urofsky v. Gilmore*, 167 F. 3d 191, 196 (4th Cir. 1999).
97. See *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
98. See 47 U.S.C. Section 223(d)(1)(B).
99. See 47 U.S.C. Section 223(a)(1)(B)(ii).
100. See 47 U.S.C. Section 231(a)(1).
101. *Id.*
102. See 47 U.S.C. Section 231(e)(2)(B).
103. See 47 U.S.C. Section 231(e)(6).
104. See Nadine Strossen, *Defending Pornography: Free Speech, Sex, and the Fight for Women's Rights* (New York: Scribner, 1995; reprint New York: New York University Press, 2000), 57–58.
105. See *American Civil Liberties Union v. Reno*, 31 F. Supp. 2d 473 (E.D. Pa. 1999).
106. *Id.*, 492.
107. See E. Chemerinsky, *Constitutional Law: Principles and Policies* (New York: Aspen Law & Business, 1997), 416.
108. See *American Civil Liberties Union v. Reno*, 31 F. Supp. 2d 473, 495 (E.D. Pa. 1999).
109. *Id.*, 497.
110. *Id.*
111. See American Civil Liberties Union, "Internet Censorship Battle Moves to Appeals Court," 1999, <http://www.aclu.org/features/f101698a.html>. *Link actually goes to:* ACLU Freedom Network, "ACLU v. Reno II Victory! Appeals Court Rejects Congress' Second Attempt at Cyber-Censorship," June 22, 2000, <http://www.aclu.org/features/f101698a.html>.
112. See *Ginsberg v. New York*, 390 U.S. 629 (1968).
113. See *Mainstream Loudoun v. Loudoun County Library*, 24 F. Supp. 2d 552 (E.D. Va. 1998).
114. See American Civil Liberties Union, "Fahrenheit 451.2: Is Cyberspace Burning?" 1997, <http://www.aclu.org/issues/cyber/burning.html>; also American Civil Liberties Union, "Censorship in a Box," 1998, <http://www.aclu.org/issues/cyber/box.html>.
115. See American Civil Liberties Union, "Censorship in A Box," 1998 <http://www.aclu.org/issues/cyber/box.html>, 9–10.
116. See *Mainstream Loudoun v. Loudoun County Library*, 24 F. Supp. 2d 552 (E.D. Va. 1998).
117. *Id.*, 567.

118. See *Harris v. Forklift Sys. Inc.*, 510 U.S. 17, 21 (1993); and Nadine. Strossen, *Defending Pornography: Free Speech, Sex, and the Fight for Women's Rights* (New York: Scribner, 1995; reprint New York: New York University Press, 2000), 119–140.
119. See *Mainstream Loudoun v. Loudoun County Library*, 24 F. Supp. 2d 552, 564–565 (E.D. Va. 1998).
120. Id. 564.
121. Id. 570.
122. Id. 567.
123. Id.
124. See D. Hedgpeth, "Libraries Abandon Court Fight; Board Won't Appeal Internet Policy Rulings," *Washington Post*, April 22, 1999.
125. For detailed information on all of these cases, including the parties' litigation papers and the courts' rulings, see the ACLU's Web site: <http://www.aclu.org/issues/cyber/hmcl.html>.
126. See Brian Gladman, "Wassenaar Controls, Cyber-Crime and Information Terrorism," Cyber-Rights and Cyber-Liberties (UK), September 1998, <http://www.cyber-rights.org/crypto/wassenaar.htm>, 4–5.
127. See National Public Radio, "Feds Say E-Mail Scrambler is a Weapon," National Public Radio Morning Edition, April 14, 1995.
128. See J. Fraser, "The Use of Encrypted, Coded and Secret Communications is an 'Ancient Liberty' Protected by the United States Constitution," *Virginia Journal of Law and Technology*, 2 (1997): 25, n.123.
129. See National Research Council, *Cryptography's Role in Securing the Information Society*, eds. Kenneth W. Dam and Herbert S. Lin, 1996, <http://www.nap.edu/readingroom/books/crisis/>, 24.
130. Ibid. 27.
131. See Global Internet Liberty Campaign, "Cryptography is a Defensive Tool, Not a Weapon," September 14, 1998, <http://www.gile.org/crypto/wassenaar/gile-statement-998.html>, 2.
132. See George Smith, "An Electronic Pearl Harbor? Not Likely," *Issues in Science and Technology Online*, Fall 1998, <http://www.nap.edu/issues/15.1/smith.htm>.
133. Ibid. 1.
134. Ibid. 2.
135. Ibid. 9.
136. Ibid. 1.
137. See The President's Commission on Critical Infrastructure Protection (Report Summary), "Critical Foundations: Thinking Differently," 1997, <http://www.info-sec.com/pccip/web/summary.html>.
138. See Andy Oram, "A Sacrifice to the War Against Cyber-Terrorism," 1997, 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 October 13, 1997 and presented by its Chairman Robert T. Marsh, before a Congressional Committee on November 5, 1997).
139. See Electronic Privacy Information Center (White Paper), "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," May 22, 1998, http://www.epic.org/security/infowar/cip_white_paper.html.
140. See Brian Gladman, "Wassenaar Controls, Cyber-Crime and Information Terrorism," Cyber-Rights and Cyber-Liberties (UK), September 1998, <http://www.cyber-rights.org/crypto/wassenaar.htm>, 4–5.
141. See Ad Hoc Group of Cryptographers and Computer Scientists, "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption," September 1998, <http://www.cdt.org/crypto/risks98/>, 15–16.
142. See Omega Foundation, "An Appraisal of the Technologies of Political Control," September 1998, <http://www.jya.com/stoa-atpc-so.htm>.
143. See Global Internet Liberty Campaign, "Cryptography and Liberty 1998," February 1998, <http://www.gile.org/crypto/crypto-survey.html> See also Electronic Privacy Information

- Center, *Cryptography and Liberty 1999: An International Survey of Encryption Policy*, 1999, <http://www2.epic.org/reports/crypto1999.html>.
144. See Global Internet Liberty Campaign, *Cryptography and Liberty 1998*, February 1998, <http://www.gile.org/crypto/crypto-survey.html>, 7.
145. See *Olmstead v. United States*, 277 U.S. 438, 479 (1928) (Brandeis, J. dissenting), overruled by *Katz v. United States*, 389 U.S. 347 (1967).

Acknowledgments An alternate version of this chapter was printed in the *International Review of Law, Computers & Technology*, 14, no. 1 (March 2000): 11–24. For research assistance with this chapter, including drafting the endnotes, Professor Strossen gratefully acknowledges her chief aide, Amy L. Tenney, and her research assistant, Cesar de Castro. The endnotes were added through the efforts of Professor Strossen's staff, who thereby have earned both the credit and the responsibility for them (which Professor Strossen has not reviewed, and for which she disclaims both credit and responsibility).