Statement of
David L. Sobel
General Counsel
Electronic Privacy Information Center

Before the
Commission on Online Child Protection

June 9, 2000
Washington, DC

Mr. Chairman and Members of the Commission:

Thank you for providing me with the opportunity to appear before the Commission to address the privacy implications of age verification technologies that might be used to restrict access to certain material on the Internet. The Electronic Privacy Information Center (EPIC), as an organization committed to the protection of both privacy rights and free expression, has a longstanding interest in this issue and has participated in relevant legislative and judicial proceedings since its inception in 1994. We also co-founded and coordinate the Internet Free Expression Alliance (www.ifea.net), a coalition of more than two dozen organizations committed to the continuation of the Internet as a forum for open, diverse and unimpeded expression with particular emphasis on both legal and technological impediments to free expression.

As an initial matter, I note that the Commission has invited me to discuss the rather limited question of whether age verification systems pose threats to personal privacy. While I welcome the opportunity to address that issue, my testimony would be incomplete if I did say a word about the underlying premise of the Commission's inquiry, namely "to identify technological or other methods that . . . will help reduce access by minors to material that is harmful to minors on the Internet." Given the inherent subjectivity of terms such as "harmful to minors" or "indecent," I believe that efforts to mandate restrictions on access to such material are prohibited by the First Amendment, particularly in a medium like the Internet, which makes content available in every community in the nation. For that reason, EPIC participated as plaintiff and co-counsel in the constitutional challenge to the Communications Decency Act and is currently acting in a similar capacity in the pending challenge to the criminal provisions of the Child Online Protection Act (COPA). Every federal judge (including the Justices of the Supreme Court) who has considered the issue has agreed that content-based restrictions on Internet "indecent" or "harmful to minors" speech are unconstitutional.

First Amendment considerations are an important aspect of my testimony today, because I believe the privacy issues we are discussing are inseparable from the free speech issues. Any requirement that Internet users identify themselves in some way (or even take additional steps to establish that they are entitled to receive the information they seek) as a condition of access to online content necessarily chills free speech. The courts have recognized that the exercise of First Amendment rights may not be conditioned upon a surrender of personal privacy. For instance, a federal appeals court invalidated a state's requirement that citizens provide their Social Security numbers when registering to vote, finding that such requirements "compel a would-be voter . . . to consent to the possibility of a profound invasion of privacy when exercising the fundamental right to vote."[1] Likewise, mandated age verification systems impose a similar condition on an adult's right to access information on the Internet. Such requirements also infringe on the First Amendment right to communicate anonymously. As the Supreme Court stated in *McIntyre v. Ohio Elections Commission*, anonymity "exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation -- and their ideas from suppression -- at the hand of an intolerant society."[2]

The privacy impacts of age verification -- and therefore the free speech implications -- are felt by both consumers and providers of online content. From a consumer perspective, a new regime for the collection of personal data in the name of "child online protection" would impose yet another burden on the privacy of Internet users. The American people, when they go online, are already acutely aware of the fact that they are being over-monitored and over-profiled. Polling results consistently show that many Americans are "concerned" or "very concerned" about the loss of privacy, particularly with regard to commercial transactions that take place over the Internet.[3] One recent poll

---

[1] *Greidinger v. Davis*, 988 F.2d 1344, 1354 (4th Cir. 1993).

[2] 115 S. Ct. 1511, 1524 (1995) (striking down an Ohio statute prohibiting anonymous distribution of campaign literature). *See also Lamont v. Postmaster General*, 381 U.S. 301, 307 (1965) (finding unconstitutional a requirement that recipients of communist literature notify the post office that they wish to receive it); *Talley v. California*, 362 U.S. 60, 64-65 (1960) (declaring unconstitutional a California ordinance that prohibited the distribution of anonymous handbills); *ACLU of Georgia v. Miller*, 977 F. Supp. 1228 (N.D. Ga. 1997) (striking down Georgia statute that would have made it a crime for Internet users to "falsely identify" themselves online).

[3] A recent poll conducted by Newsweek asked respondents how they would feel about a Web site that "tracked your movements when you browsed the site, but didn't tie that information to your name or real-world identity." Even that relatively anonymous kind of tracking led 28 percent to say they would feel "not very comfortable" and 35 percent to feel "not at all comfortable." If the site "merged your browsing habits and shopping

has indicated that the "loss of personal privacy" is the number one concern facing the United States in the twenty-first century. These results are not surprising when an Internet advertising firm such as DoubleClick reportedly has compiled approximately 100 million online user profiles to date.

Given the public concern over online privacy, it seems apparent that age verification requirements will deter most adults from accessing restricted content, because Web users are increasingly unwilling to provide identifying information in order to gain access to online content. Web users who wish to access sensitive or controversial information are even less likely to register to receive it.[4] The district court recognized this fact when it found COPA to be unconstitutional, noting that "the implementation of credit card or adult verification screens in front of material that is harmful to minors may deter users from accessing such materials."[5] Indeed, the uncontroverted evidence presented to the court established that COPA's age verification requirements would prevent or deter Web users from accessing a wide range of constitutionally protected speech.[6]

There is little doubt that all effective age verification technologies require consumers, at some stage of the verification process, to divulge personally identifiable information,

---

patterns into a profile that was linked to your real name and identity," 21 percent would feel "not very comfortable" and 68 percent "not at all comfortable." http://www.businessweek.com/2000/00_12/b3673010.htm

[4] In a related context, the Supreme Court has recognized that identification requirements can have a chilling effect on access to sexually-explicit material. In *Denver Area Educ. Telecomms. Consortium, Inc. v. FCC*, 518 U.S. 727 (1996), the Court struck down a statutory requirement that viewers provide written notice to cable operators to obtain access to certain sexually oriented programs because the requirement "restrict[s] viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the . . . channel." 518 U.S. at 754. In considering the precursor to COPA, the Supreme Court found that the credit card and adult access code requirements of the CDA would also unconstitutionally inhibit adult Web browsers. *Reno v. ACLU*, 521 U.S. at 857 n.23 ("There is evidence suggesting that adult users, particularly casual Web browsers, would be discouraged from retrieving information that required use of a credit card or password.").

[5] *American Civil Liberties Union v. Reno* ("*ACLU II*"), 31 F. Supp.2d 473, 495 (E.D. Pa. 1999).

[6] The evidence also showed that Internet users would be deterred by adult access code services that cater to the pornography industry, and would not want to affiliate with such services in order to gain access to material deemed to be "harmful to minors."

whether a credit card number, driver's license, birth certificate or other documentation. The Adult Check system, for instance, claims that it has the ability to verify independently the age of an applicant and, in order to prevent "password sharing," resorts to "originating IP address verification." While some of these technologies (such as some digital certificate systems) are less invasive than others, they all require the consumer to provide personal data to a third party.[7] On a truly voluntary basis, some consumers may choose to avail themselves of such technologies in order to conduct online transactions, and when carefully implemented they can play a useful role in facilitating electronic commerce. But any governmental mandate to obtain and use such an age verifier as a condition of access to information suffers from the constitutional defects that I have discussed.

As I have noted, the use of age verification systems impacts providers of online content as well as consumers. Given the apprehension that many consumers have about obtaining an adult ID or password, content providers who would be required to impose such requirements as a condition of access to their Web sites will suffer a loss of traffic and, consequently, revenue. Indeed, the inhibiting effect of such systems formed the basis for the district court's discussion of the issue when it considered the constitutionality of COPA:

> Evidence presented to this Court is likely to establish at trial that the implementation of credit card or adult verification screens in front of material that is harmful to minors may deter users from accessing such materials and that the loss of users of such material may affect the speakers' economic ability to provide such communications. The plaintiffs are likely to establish at trial that under COPA, Web site operators and content providers may feel an economic disincentive to engage in communications that are or may be considered to be harmful to minors and thus, may self-censor the content of their sites.[8]

The court's finding underscores the clear relationship between the privacy and free speech aspects of age verification requirements; one simply cannot be separated from the other. For that reason, such requirements would introduce a troubling new component into the Internet's architecture, one that would hasten the demise of both personal privacy

---

[7] Digital certification technologies can lessen the privacy and First Amendment implications of age verification systems, but not remove them entirely. Such approaches can separate personal identity from a particular certified characteristic; age, for instance. But they still impose upon the user the burden of providing information to the third party certificate issuer, a burden that raises constitutional problems when imposed as a condition of accessing a particular category of information.

[8] *ACLU II*, 31 F. Supp.2d at 495.

and freedom of expression. I submit that such a result is not in the long-term interests of the emerging online industry or of an American public that is increasingly turning to this medium as a vital source of information and entertainment. Rather than focus on approaches that seek to block access to information and compromise privacy, I strongly urge both the Commission and Congress to emphasis and support educational initiatives that will help young people learn to responsibly and safely navigate this exciting and enriching medium.