DOI:10.1145/3651865

James Grimmelmann

Law and Technology
The Return of Age Verification Laws

Considering the ways in which free-speech law could shift rapidly.

The most significant legal case in the history of the Internet is the U.S. Supreme Court's 1997 decision in *Reno v. American Civil Liberties Union*, which held that a federal law against online indecency was unconstitutional.[a] *Reno* was one of the earliest truly Internet-related legal cases, and it established two foundational precedents.

First, adults have a First Amendment right to speak and listen to each other, even if some of that speech is indecent, offensive, or unsuitable for children. Second, Internet services are not responsible for verifying the ages of their users, even if some children manage to see speech meant for adults. For years, these propositions were so deeply woven into the fabric of Internet law that they were often simply taken for granted.

But times change, and we are now living through the most eventful era in Internet law since the 1990s. The post-*Reno* consensus regarding how the First Amendment applies online may be unraveling. In subsequent *Communications* Law and Technology columns, I will take stock of some of the ways in which free-speech law could shift rapidly, including state social-media laws, government use of social media, and intermediary liability.

In this column, I will start by looking at a new wave of U.S. state laws that explicitly require age verification. Although these laws are inconsistent with *Reno*, some of them have been holding up in court. The story of how states drafted their new laws to get around *Reno* is a striking, perhaps even shocking, story of legal creativity.

The CDA and Reno

The first major Internet speech legislation in the U.S. was the Communications Decency Act of 1996 (CDA). As its name suggests, the CDA was intended to make the Internet family-friendly by shielding children from seeing adult content online. (Today, the CDA is most famous for including "Section 230," a broad immunity that protects Internet platforms from being held liable for user-posted content. The immunity was bundled with the anti-indecency provisions as part of a legislative compromise.)

The impetus for the CDA was a moral panic driven by the sudden arrival of the Internet in general public awareness in the 1990s. Anti-pornography activists and family-values conservatives worried that the Internet would be an unregulated free-for-all where children, both wittingly and unwittingly, could easily find uninhibited depictions and discussions of sexuality.

Public fears were fueled by an academic study that seemed to indicate the Internet was awash in pornography. It quickly emerged that the study was actually an undergraduate paper with serious methodological problems and that its conclusions had been badly misrepresented, but the damage was done. *Time* magazine ran a cover story in July 1995 featuring a small child, face bathed in the bluish glow from a computer screen, staring at the camera in wide-eyed shock.

The CDA passed the next year as

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

IMAGE BY ALICIA KUBISTA/ANDRIJ BORYS ASSOCIATES

a direct and probably inevitable response to public and political fear of online pornography. Specifically, it prohibited Internet services from showing any "obscene or indecent" or "patently offensive" content to users less than 18 years old.

Two broad coalitions of media, technology, and civil-liberties groups filed suit, alleging that the CDA was an unconstitutional restriction on freedom of speech. The case was popular among technologists and website operators, many of whom posted GIFs of a blue ribbon on their sites as a protest. It was perhaps the last time the "the Internet community" spoke with one voice about anything.

In 1997, the Supreme Court in *Reno* struck down these parts of the CDA. While laws against obscenity are allowed under the First Amendment, it protects both indecent and offensive speech for adults. The fact that speech might be harmful to minors does not necessarily make it harmful to adults, and plenty of adults willingly and legally exchange indecent speech, from dirty jokes to erotic fan fiction. The government may not "reduce the adult population ... to reading only what is fit for children."[b]

That left age verification. If a website could perfectly distinguish between children and adults, then in theory it could block children while allowing adults to read the material that was legal for them. Indeed, the CDA included a partial defense for online services that used a credit card or other identification to establish adulthood.

Reno held, however, that the theoretical possibility of using age verification could not save the CDA. Offline laws that prohibit selling cigarettes, alcohol, and pornography to minors assume, more or less correctly, that it is possible to tell children and adults apart. A storeowner can refuse to sell adult magazines to children and to people in fake mustaches. Online, however, a website has no similar screening technique to decide who gets to read the off-color jokes. Every visitor to a website is a potential minor.

b *Butler v. Michigan, 352 U.S. 380*, 383–84 (1957).

There were, and still are, three strong arguments against age-verification requirements.

Age Verification

There were, and still are, three strong arguments against age-verification requirements. The first is that they do not work. Teenagers have been presenting fake IDs to purchase beer offline for a long time, and children have been lying about their ages online for years. Minors can often get their hands on credit cards, or "borrow" someone else's credentials.

The second problem is that age verification is a serious burden on speech. Even a simple "What is your birth date?" splash page takes effort

to implement and will deter some users who are legally allowed to visit. Anything more secure is correspondingly more expensive and will block legitimate visitors. Anyone who has ever tried to order from an e-commerce site that expects payment using a different country's payment card is familiar with the these burdens.

Third, age-verification infrastructure creates privacy burdens. To certify a user is an adult, an age-verification service needs to verify their identity (and thus their online activity) against governmental records. For sensitive topics—such as sexuality, whistleblowing, political dissent, or religion, to name just a few—this linkage by itself can have a chilling effect on speaking and reading. Alternative systems that promise to use biometrics to verify age also rely on sensitive, regulated data.

The general consensus against mandatory age verification defined by *Reno* held for two decades. But a new crop of state laws harkens back to the CDA's pre-*Reno* attitude that some online content is inherently harmful to children. The same ongoing moral panic about sexuality that is leading some states to prohibit gender-affirming medical care and to remove books from library shelves has also led numerous states to enact laws that prohibit children from using social media or accessing adult content.

This new crop of laws either explicitly or effectively require age verification. Although there is some variation from state to state, they typically prohibit social-media companies from serving minors without parental consent. Some go further and require that the age cutoff be backed up with third-party age verification based on driver's licenses or similar identification.

It would seem that these laws are unconstitutional under *Reno*. But although some of them have been struck down in litigation,[c] federal courts have dismissed lawsuits against others.[d] (Many of these decisions are currently on appeal.)

c For example, *NetChoice, LLC v. Griffin,* No. 5:23-CV-05105 (W. D. Ark. Aug. 31, 2023).

d For example, *Free Speech Coalition v. Anderson*, No. 2:23-CV-287 (D. Utah Aug. 1, 2023).

Some of these laws have managed to evade scrutiny through a drafting trick: They are not enforced by state officials.

Manipulating the Judicial System

Some of these laws have managed to evade legal scrutiny through a drafting trick: They are not enforced by state officials. Instead, they rely on private plaintiffs. The Louisiana law, for example, says services "shall be liable to an individual for damages resulting from a minor's accessing the material." The idea is that a minor's parents who catch their child viewing content they disapprove of could sue the service that allowed the minor to sign up.

This drafting choice may seem bizarre, but there is a calculated logic behind it. The key is that a company or industry suing to block a state law only has "standing" to sue in federal court the people who would actually enforce that law. For traditionally drafted laws, such as the CDA, that means governmental officials, who can be identified and served with the lawsuit. But for private-plaintiff laws like Louisiana's, the enforcer could literally be any "individual." The courts in these cases have held that Internet companies do not have standing to sue state officials. Instead, they have to wait until some "individual" comes forward to enforce the law, and then raise their constitutional objections as a defense in that lawsuit.

In theory, the First Amendment and *Reno* should protect Internet companies here. They can wait to be sued, then raise a First Amendment defense and win. But this approach comes with immense risk. The only way to win one of these cases is to provide service to thousands or millions of people and wait for one of them to decide to sue. If the company loses that lawsuit, it could face immense liability from thousands of other plaintiffs. Even if the odds are good overall and the damages from any one lawsuit are small, a moderate chance of a huge judgment is a catastrophic risk.

This drafting trick is not new. Texas used a private-plaintiff law to outlaw abortion in the state even before the Supreme Court held in *Dobbs v. Jackson Women's Health Organization* that there is no constitutional right to abortion.[e] It was an effective way to push the boundaries of the Constitution. Although abortion clinics in Texas had a good chance of winning any of these cases, there was too much of a chance they might lose.

Without the ability to protect their rights by bringing a challenge against an unconstitutional law before it was enforced against them, the abortion clinics effectively lost those rights. The same thing is happening to Internet companies now in states with private-plaintiff age-verification laws. Some pornography companies have stopped providing service in these states altogether, and other companies are adopting age verification.

Laws that are quite likely unconstitutional are changing behavior on the ground, and they are changing it in ways that erode the constitutional argument against them. The more widely used that age verification becomes, the weaker the argument that it is an undue burden on speech or that it is unreliable. Every provider who acquiesces rather than take the risk of being sued makes it more difficult for others to stand on their rights. If every company complies, then no private plaintiff will sue, and there will never be an opportunity for the courts to decide whether these laws are constitutional. *Reno* remains good law on the books, but there is a serious danger it might become irrelevant on the Internet. C

e *Dobbs v. Jackson Women's Health Organization*, 142 S. Ct. 2228 (2022).

James Grimmelmann (james.grimmelmann@cornell.edu) is the Tessler Family Professor of Digital and Information Law at Cornell Tech and in the Law School at Cornell University, New York, NY, USA.