AMERICAN CIVIL LIBERTIES UNION OF GEORGIA V. MILLER

By Patrick Weston

Although it is becoming trite to say so, hardly anyone would dispute that the Internet is changing society.[1] As industrialized societies embrace and make use of the many benefits of this new technology, however, new issues and challenges emerge.

One such challenge is dealing with the ways in which the Internet can be used to facilitate fraud. The Internet enables a would-be perpetrator to come into contact with millions of people with much greater ease and much less cost than ever before. It further allows people to communicate and transact business in a world where identities are no longer apparent or easily verifiable, where transactions can be consummated at high speed, and where entities whom one encounters can be ephemeral and impossible to locate again.

In an attempt to confront these new issues, various governmental bodies are in the process of crafting new laws to protect society from the perceived dangers that this technological shift brings.[2] However, many of the early legislative responses to address the threat of crime on the Internet were drafted incautiously and have run into constitutional difficulties.[3] Statutes that attempt to regulate behavior on the Internet need to be drafted with sophistication, both to accomplish their purpose and to pass constitutional muster.

---

1. "The Internet is a network of networks—a decentralized, self-maintaining series of redundant links among computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control. No organization or entity controls the Internet; in fact, the chaotic, random structure of the Internet precludes any exercise of such control." American Libraries Assoc. v. Pataki, 969 F. Supp. 160, 164 (S.D.N.Y. 1997).

2. *See generally* American Civil Liberties Union, *Online Censorship in the States* (last modified Mar. 25, 1998) <http://www.aclu.org/issues/cyber/censor/stbills.html> (citing examples of various attempts by states to regulate the Internet).

3. *See, e.g.*, American Civil Liberties Union v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997) (striking down most of the Communications Decency Act); *Pataki*, 969 F. Supp. 160 (striking down a New York law prohibiting the distribution of material harmful to minors over the Internet); ACLU of Ga. v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997) (striking down a Georgia act prohibiting anonymity on the Internet).

In *ACLU of Georgia v. Miller*,[4] the U.S. District Court for the Northern District of Georgia enjoined that state from enforcing legislation aimed at preventing fraud on the Internet because the legislation was overbroad, vague, and not narrowly tailored to achieve a compelling state interest.[5] The court looked only to these factors in its succinct opinion because it found them sufficient cause to issue a preliminary injunction. However, there are additional reasons that make the Georgia legislation constitutionally flawed, and these reasons must be considered to achieve success with future Internet legislation. This Note examines the court's decision, as well as additional considerations presented by the Georgia legislation, and attempts to provide a framework for drafting legislation in the future.

I. BACKGROUND

In early 1996, the Georgia legislature enacted a statute that endeavored to address fraud on the Internet. Georgia House Bill 1680, officially entitled the Georgia Computer Systems Protection Act ("the Act")[6] was passed in an attempt to combat "computer related crime," which the legislature found to be a "growing problem in the government and in the private sector."[7]

Many of the Act's provisions deal with crimes such as the unlawful theft or alteration of computer records and the unauthorized use of computer facilities. However, one section of the Act makes it illegal to "knowingly ... transmit any data through a computer network ... for the purpose of setting up, maintaining, operating, or exchanging data with an electronic mailbox, home page, or any other electronic information storage bank or point of access to electronic information" if such data is misleading.[8] The Act defines "misleading" data as either (1) data that "uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data," or (2) data that falsely implies that the sender has permission to use a trade name or other official mark.[9] Moreover, the Act contains a sweeping venue provision that allows an ac-

4. 977 F. Supp. 1228 (N.D. Ga. 1997).
5. *See id.* at 1234-35.
6. GA. CODE ANN. § 16-9-90 (1996).
7. GA. CODE ANN. § 16-9-91 (1996).
8. GA. CODE ANN. § 16-9-93.1 (1996).
9. *See id.*

tion to be brought in "any county from which, to which, *or through which*"[10] any prohibited computer transmission was made.

Ostensibly, the ban against transmitting the first kind of misleading data combats fraud by preventing individuals from disguising their identities, or even acting anonymously, with respect to Internet communications. Similarly, the ban against the second kind of data is designed to protect copyright and trademark holders from the unauthorized use of their names and symbols.

II. THE DISTRICT COURT DECISION

On September 24, 1996, a group of plaintiffs led by the American Civil Liberties Union filed suit to have the Georgia law overturned.[11] They alleged that the Act was an infringement of their First Amendment rights, that it was overbroad, that it was impermissibly vague, and that it imposed an unconstitutional burden on interstate commerce in violation of the Commerce Clause of the United States Constitution.[12] The District Court granted a preliminary injunction, enjoining Georgia from enforcing section 16-9-93.1 of the Georgia Code.[13]

After finding the defendants' affirmative defenses to be unpersuasive,[14] the court considered the merits of three of the plaintiffs' claims. The court reasoned that because "the identity of the speaker is no different from other components of [a] document's contents that the author is free to include or exclude,"[15] the statute's prohibition of Internet transmissions

---

10. GA. CODE ANN. § 16-9-94(4) (1996) (emphasis added).

11. *See* ACLU of Ga. v. Miller, 977 F. Supp. 1228, 1228 (N.D. Ga. 1997).

12. *See* J. Scott McClain, *Plaintiffs' Complaint,* ACLU v. Miller, *Civil Action No. 1:96-cv-2475-MHS* (visited Oct. 14, 1998) <http://www.aclu.org/issues/cyber/censor/GACOMPLT.html>.

13. *See Miller*, 977 F. Supp. at 1235.

14. The defendants asserted two affirmative defenses: (1) that the plaintiffs lack standing to bring this action because they have not been prosecuted or threatened with prosecution, and (2) that the federal court should abstain from exercising jurisdiction because the law is ambiguous and in need of state court interpretation. However, the court found that plaintiffs do have standing because a credible threat of prosecution exists, and the rules of standing are relaxed in the First Amendment context where the alleged danger is one of self-censorship. The court also found that the Georgia statute was not subject to any limiting construction by a state court that would overcome its constitutional problems, and that abstention would impose a great burden on the plaintiffs by chilling their expression while they waited for a state court interpretation. Thus, the court decided that abstention was inappropriate in this case. *See id.* at 1231-32.

15. *Id.* at 1232 (citing McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 340-42 (1995)).

which "falsely identify" the sender constitutes a presumptively invalid content-based restriction.[16] In order to overcome this presumption of invalidity, defendants must demonstrate that the statute furthers a compelling state interest and is narrowly tailored to achieve that interest.[17] The court agreed with the defendants that fraud prevention is a legitimate state interest.[18] However, because the criminal prohibition applies whether or not a speaker has any intent to deceive or whether or not deception actually occurs, the court found that the statute was not narrowly tailored to meet that interest.[19] Instead, the court found that the statute "sweeps innocent, protected speech within its scope."[20]

The defendants claimed that a variety of limiting concepts that narrow the scope of the statute should be included when interpreting it, but the court rejected the contention that intent requirements could be subsequently 'grafted' on to it when they did not appear in the language of the statute.[21] The court also rejected the defendants' contention that the Act only applies to those who misappropriate the identity of another specific entity or person, noting that there is nothing in the language of the Act from which such a requirement could be reasonably inferred.[22]

The court thus concluded that the statute is not readily susceptible to a limiting construction and that the plaintiffs would likely prevail on their claim that the statute by its plain language imposes content-based restrictions that are not sufficiently tailored to promote a compelling state interest.[23]

The court also concluded that the statute was not drafted narrowly or precisely enough for a law that regulates speech because, on its face, the Act proscribes such protected speech as "[t]he use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy, as well as the use of trade names or logos in non-commercial educational speech, news, and commentary...."[24] This gives rise to recognized First Amendment problems because even if the statute

16. *See id.* (citing R.A.V. v. St. Paul, 505 U.S. 377, 382 (1992)).

17. *See id.* (citing Sable Communications of California, Inc. v. FCC, 492 U.S. 115, 126 (1989)).

18. *See id.*

19. *See* ACLU of Ga. v. Miller, 977 F. Supp. 1228, 1232 (N.D. Ga. 1997).

20. *Id.*

21. *See id.*

22. *See id.* Contrary to the defendants' contention, the wording of the statute prohibits not only stealing another person's name, but also inventing a pseudonymous name for oneself.

23. *See id.* 1233.

24. *Id.*

could properly be used to prosecute those who commit outright fraud, it still operates unconstitutionally for a substantial portion of the speakers it covers.[25]

Finally, the court found that the plaintiffs were likely to succeed on their claim that the Act is unconstitutionally vague because the statute "(1) does not give fair notice of the conduct it proscribes; (2) is conducive to arbitrary enforcement; and (3) infringes upon plaintiffs' free expression."[26] The Act does not give fair notice because key terms such as "falsely identify," "use," "falsely imply," and "point of access to electronic information" are undefined in the statute.[27] The Act also creates the risk of arbitrary enforcement because it fails to notify law enforcement officials of exactly what conduct is prohibited—affording police and prosecutors considerable room for selective prosecution of persons who express minority viewpoints.[28] The Act is especially harmful, however, because it chills protected expression: due to plaintiffs' inability to discern what exactly the act prohibits, they are forced to restrict legitimate behavior, and this self-censorship would continue without court intervention.[29]

The court thus felt that the plaintiffs were likely to prevail on these three claims and granted a preliminary injunction against state enforcement of Georgia Code Section 16-9-93.1.[30] The court noted that "the public interest weighs in favor of having access to a free flow of constitutionally protected speech."[31]

III. DISCUSSION

A. Issues Presented by the Internet

Fraudulent practices crop up in the online world just as they do in other aspects of our lives. To some extent, these cyberspace abuses are merely on-line versions of more conventional mail and telephone scams.[32]

---

25. *See* Village of Shaumburg v. Citizens for a Better Environment, 444 U.S. 620, 634 (1980); ACLU of Ga. v. Miller, 977 F. Supp. 1228, 1233 (N.D. Ga. 1997).

26. *See Miller*, 977 F. Supp. at 1234.

27. *See id.*

28. *See id.*

29. *See id.*

30. *See id.* at 1234-35.

31. *Id.* at 1235 (citing American Civil Liberties Union v. Reno, 929 F. Supp. 824, 851 (E.D. Pa. 1996)).

32. For example, pyramid schemes and chain letters are just as easy to propagate through e-mail as they are through traditional mail. *See generally* Jo-Ann M. Adams, *Controlling Cyberspace: Applying the Computer Fraud and Abuse Act to the Internet*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 403, 408-15 (1996).

However, the Internet's unique characteristics have also been exploited to perpetrate new types of fraudulent harms.

The characteristics that tend to make online consumer abuse unique and, perhaps, more challenging to confront than fraudulent activities associated with more traditional means of communication are the same characteristics that give the Internet its strength. One commentator has suggested that there are four such inherent characteristics of the Internet: (1) accessibility, (2) anonymity, (3) transience, and (4) interactivity.[33] Exploring these characteristics and coming to an understanding of how they function provides a solid foundation from which to analyze the shortcomings of the Georgia legislation and to suggest how Internet legislation could be better drafted in the future.

1. Accessibility

Practically anyone with a computer and a phone line can obtain access to the web and an e-mail address.[34] Once an e-mail address is established, it is possible for a user to send and receive substantially unlimited numbers of messages without paying any additional fees. Moreover, there are easily accessible programs that enable the same message to be sent to thousands of recipients with merely a few keystrokes. For example, virtually anyone can send sales information to countless potential buyers (or victims) cheaply and with ease. Similarly, practically anybody can set up a web page and place content on the Internet for anyone else to see.[35]

As a result, the Internet makes it possible for a person to disseminate information to millions of other users almost effortlessly and at little or no cost. Unlike traditional media, the barriers to entry as a speaker on the Internet do not differ from the barriers to entry as a listener.[36] In other words, traditional mass-communications media like newspapers or television make it very easy for one to receive information, but it is very expensive for an individual to utilize them to disseminate information. Tradi-

---

33. *See* Barry Fraser, *Regulating the Net: Case Studies in California and Georgia Show How Not To Do It*, 9 LOY. CONSUMER L. REP. 230, 235 (1997).

34. Indeed, many services such as Hotmail and Juno (among others) offer free e-mail addresses to anyone who wants them. *See, e.g.*, Juno, *Juno Home Page* (visited Feb. 20, 1999) <http://www.juno.com/>; MSN Hotmail, *The World's FREE Web-Based Email* (visited Feb. 20, 1999) <http://www.hotmail.com/>.

35. Some companies like GeoCities even offer free space for users to create web pages. *See, e.g.*, GeoCities, *Home Pages & Beyond* (visited Feb. 20, 1999) <http://www.geocities.com/>.

36. *See* American Civil Liberties Union v. Reno, 929 F. Supp. at 843; *see also* Ian C. Ballon, *The Law of the Internet: Developing a Framework for Making New Law (Part 1)*, 2 CYBERSPACE L. 12 (1997).

tionally, in order to reach such large numbers of people one had to incur large costs in the form of print media advertising to a national/worldwide audience, direct phone solicitation, direct mail campaigns, or other similar methods. For example, corporations have paid over a million dollars for a few seconds of television airtime to send a message to the viewing audience of the Super Bowl.[37] When using the Internet, on the other hand, an individual can receive information from, or send information to, millions of people for the same miniscule cost.

2. Anonymity

It is quite simple for users of the Internet to communicate or exchange information anonymously or under a pseudonymous identity.[38] Many e-mail addresses and web sites contain little, if any, information that reveals the true identity or physical location of their owners.[39] Moreover, the use of "anonymous remailers" allows Internet users to obscure further their true identities by having all identifying information stripped from electronic messages before they reach their recipients.[40]

There are many advantages to the ability to communicate anonymously in cyberspace. Anonymity allows users to espouse unpopular ideas without fear of retaliation, victims of crime or disease are able seek advice without stigma, and citizens can freely engage in political speech without identifying themselves to those in power.[41] Additionally, anonymity helps users maintain their privacy and security, as well as prevent the amassing of personal information about them, such as their viewing or shopping habits on the Internet.[42]

However, anonymity poses problems as well. Because it allows users to hide their true identities, they can do great harm to others without being

---

37. Thirty-second advertising spots during the 1998 Super Bowl cost $1.3 million on average. *See* Tammi Wark, *Milestones That Marked Our Year: What Will 1998 Be Remembered For?*, USA TODAY, Dec. 30, 1998, *available in* 1998 WL 5745984.

38. *See generally* Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117 (1996).

39. *See* J. Scott McClain, *Plaintiffs' Complaint,* ACLU v. Miller, *Civil Action No. 1:96-cv-2475-MHS* (visited Oct. 14, 1998) <http://www.aclu.org/issues/cyber/censor/GACOMPLT.html>. *See also* Reno v. American Civil Liberties Union, 117 S. Ct. 2329, 2337 n.20 (1997) ("An e-mail address provides no authoritative information about the addressee, who may use an e-mail 'alias' or an anonymous remailer. There is no universal listing of e-mail addresses and corresponding names or telephone numbers, and any such listing would rapidly become incomplete.") (internal citations omitted).

40. *See* McClain, *supra* note 39.

41. *See id.*

42. *See id.*

held accountable.[43] "Law enforcement officials or lawyers seeking to file a civil suit might not be able to identify an individual to hold responsible."[44] Indeed, this problem can become especially troublesome to consumers because it provides an easy way for fraudulent business to be transacted with almost no direct means of accountability.

Imagine, for example, that in order to buy a product in the real world you had to hand cash to someone you did not know in a car with tinted windows and no license plates, who would then drive away promising that your purchase would arrive by mail next week. If the product then failed to arrive, what recourse would you have? Practically none—which is exactly why most people would think it extremely foolish to transact business in this fashion. In some fundamental ways, buying goods on the Internet is not that much different: it is not necessary for a sales site to have a physical store location, an address, a phone number, or face-to-face contact when transacting business. As a result, it can be very difficult for the buyer to find an avenue of recourse if the transaction goes sour. It is true that most successful commerce sites are not so anonymous, otherwise wary customers would avoid them. However, the potential does certainly exist for imprudent users to be defrauded.

3. Transience

Any web page or e-mail address can be changed or removed by its owner without notice to other users of the Internet.[45] Furthermore, a user can easily maintain multiple e-mail addresses and web sites and can duplicate them or change their location with minimal effort. The transient nature of the Internet has the two-fold effect of making the Internet both an energetic and stimulating place to exchange information, and a haven for malefactors who want to cover their tracks and avoid capture.

As a simple example, a person operating a fraudulent business on the Internet could operate numerous similar sites simultaneously. Then, if a victim visited one of these sites and later attempted to find out who deceived her, it would be nearly effortless for the web-site owner to make that particular site disappear completely—while at the same time creating

---

43. *See* Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1642-43 (1995).

44. *Id.*

45. Although some are endeavoring to make and maintain massive archive copies of the entire web, even arguably the most ardent supporter of such a project concedes that it may never be practical or possible to keep a copy of all the data available on the Internet. *See* Brewster Kahle, *Archiving the Internet* (last modified Mar. 2, 1998) <http://www.archive.org/sciam_article.html>.

another site somewhere else to carry on the shady transactions. Hence, the transient nature of the Internet can eliminate much of the evidence trail and the costs of physical relocation which would burden a fraudulent operation in more traditional marketplaces.

4. Interactivity

The Internet provides a way for users to communicate in real time, unburdened by physical distance, and to exchange a wealth of information with only a few keystrokes. This interactivity makes the Internet ideally suited for electronic commerce because it allows consumers to find information and conduct business transactions almost instantaneously—from any location and at any time. Despite its benefits, the interactivity of the Internet also makes it conducive to fraud because it is very easy for the unsophisticated user to disclose personal or financial information to unknown or anonymous parties who may fraudulently use such information.

The interactivity of the Internet allows entire transactions, from offer and acceptance to payment, to be completed with a few mouse-clicks. Transactions can occur immediately, and the buyer's credit card or bank account can be debited within seconds.[46] Indeed, forms of "cybercash" are emerging that can be used to make payments and bypass traditional credit card companies and financial institutions altogether.[47] Because the whole transaction can happen so quickly, there is no delay to protect a buyer from making a hasty or uninformed purchase, nor is there any grace period for the buyer to change his mind or to verify the quality of the product.[48] For example, it is easy to use the Internet to purchase anything from a book to airline tickets to an expensive computer system. Thus, while the interactivity of the Internet benefits consumers by reducing the cost and time needed to transact business, this characteristic also inherently removes some of the protections that consumers have traditionally relied on, making consumers more vulnerable to fraud.

---

46. *See id.*

47. *See generally* Simson Garfinkel, *Dumb Money* (visited Jan. 30, 1999) <http://www.hotwired.com/packet/garfinkel/96/44/geek.html>.

48. *See* Fraser, *supra* note 33, at 238 (citing Consumer Protection Policy, 425 Trade Reg. Rep. (CCH) F.T.C. Staff Report Vol. II, 22 at 28-29 (June 12, 1996), *also available at* <http://www.ftc.gov/WWW/opp.global.htm> (visited Sept. 23, 1998)).

B. Internet Regulation Needs to Be Narrowly Tailored to Address Specific, Harmful Conduct While Not Proscribing Useful Or Protected Conduct

The first problem with the Georgia Act is that a requirement of malicious intent is absent for the conduct that it proscribes. The proponents of the Georgia Act claim that it does not outlaw all anonymous communications or all uses of pseudonyms, but only fraudulent computer use where such behavior makes it troublesome to hold wrongdoers accountable.[49] However, the Act contains no limitations that require deceptive intent or practice. On its face, the Act "prohibits such protected speech as the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy, as well as the use of trade names or logos in non-commercial educational speech, news, and commentary—a prohibition with well-recognized first amendment problems."[50]

The Act is overbroad because it "sweeps protected activity within its proscription."[51] As a result, the court concluded that the statute was not "drafted with the precision necessary for laws regulating speech."[52] Thus, even if the statute would serve the state's purported interest in preventing certain types of fraud, it is still overbroad because it functions unconstitutionally for a substantial number of the speakers and activities it covers.[53]

The right to publish and speak anonymously is a right that dates back to the founding of our country. One commentator has noted, "At the time the first amendment was adopted, the device of anonymous political authorship was well known, and utilized by many of the founding fathers."[54] The Supreme Court has recently re-affirmed the constitutional right to anonymity in *McIntyre v. Ohio Elections Commission*,[55] stating that "[a]nonymous pamphlets, leaflets, brochures and even books have

---

49. *See generally Brief in Opposition to Plaintiff's Motion For Preliminary Injunction,* ACLU of Ga. v. Miller *(No. CIV.A.1:96CV2475MHS)* (visited Oct. 2, 1998) <http://www.inteliview.com/aclubpi.txt>.

50. ACLU of Ga. v. Miller, 977 F. Supp. 1228, 1233 (N.D. Ga. 1997).

51. M.S. News Co. v. Casado, 721 F.2d 1281 (10th Cir. 1983) (citing Erznoznik v. City of Jacksonville, 422 U.S. 205, 212-13 (1975)).

52. *Miller*, 977 F. Supp. at 1233.

53. *See id.* (citing Village of Schaumberg v. Citizens for a Better Environment, 444 U.S. 620, 634 (1980)).

54. Comment, *The Right to Anonymity*, 70 YALE L.J. 1084, 1085 (1961). Indeed, anonymous speech played an important role in the founding of our country: Thomas Paine wrote his momentous pamphlet "Common Sense" under a pseudonym, and the Federalist Papers, published during the debates surrounding the formation of the Constitution, were published anonymously.

55. 514 U.S. 334 (1995).

played an important role in the progress of mankind.... Persecuted groups and sects from time to time have been able to criticize oppressive practices and laws either anonymously or not at all."[56] The Court went on to state that not "all anonymous publications are pernicious," and that First Amendment freedoms cannot be nullified because of anonymity alone.[57]

The Court held that prohibiting anonymity is a content-based regulation because "the identity of the speaker is no different from other components of the document's content that the author is free to include or exclude."[58] On two other occasions, the Supreme Court held that "content-based restrictions are presumptively invalid,"[59] and that the government may regulate the content of protected speech only to promote a "compelling interest" and only "if it chooses the least restrictive means to further the articulated interest."[60]

Therefore, by endeavoring to prohibit all anonymous activity and not just harmful anonymous activity, the Georgia Act violates First Amendment protections. If the Act was aimed at preventing all anonymous speech on the Internet, then Georgia clearly lacks a compelling state interest and runs afoul of the Constitution. If, on the other hand, Georgia genuinely desired to prevent Internet fraud, then the legislature should have been more specific in the wording of the statute.

Although the Supreme Court said in *McIntyre* that anonymity per se could not be outlawed, it left open the question of whether a law prohibiting anonymity that was narrowly-tailored to prevent fraud and deception might survive a First Amendment challenge.[61] Like the Georgia Act, the Ohio statute that was struck down in *McIntyre* contained no language that indicated it was solely intended to prevent malicious uses of anonymity. The court's finding in *Miller* that the Georgia statute was vague and overbroad, as well as its reliance on *McIntyre*, suggests that a narrowly-tailored statute, which prohibits anonymity only when used injuriously,

---

56. *Id.* at 341-42 (striking down an Ohio statute prohibiting anonymous distribution of campaign literature, and quoting Talley v. California, 362 U.S. 60, 64 (1960), which declares unconstitutional a California ordinance that prohibited the distribution of anonymous handbills).

57. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341 (1995).

58. *Id.* at 348.

59. R.A.V. v. St. Paul, 505 U.S. 377, 382 (1992).

60. Sable Communications of California, Inc. v. FCC, 492 U.S. 115, 126 (1989).

61. *See McIntyre,* 514 U.S. at 343-44. See also Justice Ginsburg's concurrence, which states that while Ohio lacked cause for inhibiting the anonymous political leafletting at issue, "[w]e do not thereby hold that the State may not in other, larger circumstances, require the speaker to disclose its interest by disclosing its identity." *Id.* at 358 (Ginsburg, J., concurring).

might serve a sufficiently compelling interest to survive First Amendment scrutiny. Although it remains untested in the courts, a change in the law as basic as inserting a malicious intent requirement to make anonymous communication illegal could be enough to allow the law to serve a compelling interest, and be sufficiently narrowly tailored to be constitutional.

When drafting future legislation aimed at preventing crime on the Internet, then, lawmakers should not constrain the characteristics of the Internet that make it a unique form of communication (such as anonymity). Instead, future legislation should focus on outlawing the application of these qualities for criminal or harmful purposes. In this way, it can target the behavior that is criminal and serve a compelling interest without being too broad and proscribing harmless, protected speech.

C. Internet Regulation Needs to Be Well-Defined And Clearly Drafted so that Proscribed Conduct will Be Readily Apparent

The Georgia Act as written also presents problems under the void-for-vagueness doctrine.[62] Under this doctrine, a statute is unconstitutionally vague if it does not "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement."[63]

Because the Act fails to define key terms, it fails to give satisfactory notice of the scope of prohibited conduct to ordinary people. For instance, reasonable minds could differ as to the meaning of a "point of access to electronic information." Is it a computer linked to the Internet? A fax machine? A telephone? The Georgia legislature probably would not attempt to go so far as to say everyone must positively identify themselves when placing a simple phone call, but it is evident that the wording of the Act can lead to confusion. This ambiguity also creates a risk of arbitrary enforcement because it fails to advise law enforcement officials of exactly what conduct is illegal, thus opening the door to the evil of selective enforcement.

The Act's vagueness is especially injurious because it chills protected expression. Because it is not clear exactly what conduct is prohibited, users are forced to resort to self-censorship, and to refrain from some faultless and legitimate behaviors to avoid the threat of prosecution. Future legislation could avoid this problem quite simply by using clearer drafting and terminology that is more precisely defined. Rather than use vague

62. *See* ACLU of Ga. v. Miller, 977 F. Supp. 1228, 1234 (N.D. Ga. 1997).
63. *Id.* (citing Kolender v. Lawson, 461 U.S. 352, 357 (1983)).

terms to refer to a myriad of developing technologies and leave the interpretation up to the courts, statutes must either use more precise terms, such as "e-mail," "web page," "on-line commercial transaction," and "Internet server," or explicitly define the terms that they do use so that there is no confusion as to what conduct is prohibited.

Although those with technical backgrounds will protest that these terms are not absolutely precise themselves, such terms are nonetheless much clearer than language such as "any point of access to electronic information." For example, confusion could be eliminated if the law instead said something like, "It shall be illegal, with the intent to defraud, either to send anonymous e-mail messages or maintain web sites that do not clearly identify the owner."

D. Internet Regulation Needs to Be Drafted so as not to Place Undue Burdens on the Entire Country/World

Although the court in *Miller* did not reach this issue, it is highly likely that the Georgia Act also runs afoul of the Commerce Clause of the United States Constitution[64] because it restricts online communications occurring entirely outside the state of Georgia.[65] The Act's venue provision authorizes prosecutions in any Georgia county "from which, to which, *or through which* any [prohibited] use of a computer or computer network was made."[66] This presents a number of problems.

First, the Act restricts communication from anywhere in the world that takes place in an online public forum because these online forums can be accessed by users in Georgia.[67] If, for example, a user in Oregon posts a message to an Internet discussion group under a pseudonym, another user in Georgia may access and read that message—thereby subjecting the Oregon author, posting her message in Oregon, to prosecution in Georgia.

Second, the Act affects direct communication between people entirely outside Georgia, because the nature of the Internet is such that a message may follow any of hundreds of unpredictable routes between various computers to get to its intended recipient. It is entirely possible that, completely unknown to the sender or the receiver (who could be anywhere in

64. U.S. CONST. art. I, § 8.

65. *See Brief in Support of Motion for Preliminary Injunction*, ACLU v. Miller (last modified Dec. 11, 1997) <http://www.aclu.org/issues/cyber/censor/GABRIEF.html> (visited on Oct. 14, 1998) [hereinafter *ACLU's Brief*].

66. Ga. Code Ann. § 16-9-94(4) (1996) (emphasis added).

67. *See ACLU's Brief*, *supra* note 65.

the world), a given message may have passed through some computer or wire somewhere in Georgia, placing both parties at risk of prosecution.[68]

Third, it is practically impossible to determine the specific geographic location of a site on the world wide web. Hence, the Act affects the ability of any online user to access web pages anonymously for fear that the site they are accessing might, unbeknownst to them, be located on a computer in Georgia and subject them to prosecution as a result.[69]

Finally, the Act affects the ability of any person to *publish* a page on the web, regardless of where she lives, because there is no realistic way to prevent someone in Georgia from accessing her site. As a result, a web publisher anywhere in the world must comply with the Georgia Act's restrictions or risk prosecution.[70]

Thus, the wording of the statute clearly places many burdens on online users regardless of where they live. Any Internet user must comply with the terms of the Georgia statute or risk prosecution in Georgia, even if they had no knowledge or intent that their communication was passing through, or being read in Georgia. Because the Act applies to all interstate Internet communications (including business transactions) that merely pass through Georgia, the law essentially has the effect of regulating a sizable amount of activity occurring entirely outside the state, and is most likely in violation of the dormant Commerce Clause.[71]

The dormant Commerce Clause may preclude the entire field of online communications from state regulation.[72] Because information on the Internet flows between computers without regard to geographic boundaries, any regulation of online communication by one state could very easily apply to users everywhere. And if states imposed different regulations on online communications, every user would be subject to conflicting standards because online information is accessible from—and could travel

---

68. *See id.* As a basic example, if one person in California sends an e-mail message to another person in California, there is no way of predicting which computers or wires it will pass through to get from the sender to the receiver. Unbeknownst to either of them, the message could briefly pass through a computer in Georgia along the way, and subject both parties to criminal prosecution there even though they are both in California!

69. *See id.*

70. *See id.*

71. When a state statute directly regulates interstate commerce, the Supreme Court has generally "struck down the statute without further inquiry." Brown-Forman Distiller's Corp. v. New York State Liquor Auth., 476 U.S. 573, 579 (1986). *Accord* Healy v. Beer Institute, 491 U.S. 324, 336 (1989); Edgar v. MITE Corp., 457 U.S. 624, 643 (1982); Baldwin v. G.A.F. Seelig, Inc., 294 U.S. 511, 521 (1935).

72. *See ACLU's Brief, supra* note 65.

through—every state in the nation.[73] Under this theory, online communications would be precluded from state regulation because "[t]he Internet is one of those areas of Commerce that must be marked off as a natural preserve to protect users from inconsistent [state] legislation that, taken to its most extreme, could paralyze the development of the Internet altogether."[74]

Perhaps the solution to this problem is for a state to draft its laws such that they only apply to people who are physically located in (that is, send information from, or access information while in) that state. Admittedly, this is an imperfect solution because someone could evade such a law by merely re-locating in another state. A more palatable solution might be for the federal government to exercise its Commerce Clause powers and promulgate federal laws that regulate conduct on the Internet, so that there is a uniform national standard and method for confronting the necessarily interstate problem of computer fraud.[75] The court in *American Libraries Association v. Pataki*,[76] following this theory, stated that "the Commerce Clause ordains that only Congress can legislate in [the area of Internet regulation], subject, of course, to whatever limitations other provisions of the Constitution (such as the First Amendment) may require."[77] Indeed, there already is some federal response to the problem of fraud on the Internet: the Department of Justice has a computer crimes unit that investigates online crimes, the Federal Trade Commission monitors online advertising and commercial services, and the Securities and Exchange Commission watches financial chatter in cyberspace.[78]

---

73. *See generally* CTS Corp. v. Dynamics Corp. of Am., 481 U.S. 69, 88 (1987); *accord* American Libraries Ass'n v. Pataki, 969 F. Supp. 160 (1997) (holding that a New York statute making it a crime to use a computer to disseminate obscene material to minors violated the Commerce Clause).

74. American Libraries Assoc. v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997). For other examples of channels of interstate commerce exempt from state regulation, see, e.g., Southern Pacific Co. v. Arizona, 325 U.S. 761 (1945) (finding the length of train cars exempt from state regulation), and Wabash St. L & P Ry. Co. v. Illinois, 118 U.S. 557 (1886) (holding railroad rates exempt from state regulation).

75. We already have federal statutes that deal with wire fraud, mail fraud, interstate transportation of stolen goods, etc. In addition, see the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, which could be utilized to provide a federal solution for combating crime on the Internet. *See generally* Adams, *supra*, note 32, at 420-31.

76. 969 F. Supp. 160 (S.D.N.Y. 1997).

77. *Id.* at 169.

78. *See* Claire Ann Koegler, *The Information Highway Patrol: Here Come the Cybercops*, 22 NOVA L. REV. 513, 525-26 (1998).

IV. CONCLUSION

As one commentator has said, "Although the Georgia Act does succeed in identifying anonymity, accessibility, and transience as the basis for many consumer harms, it tries to deter these harms by prohibiting activities that are essential to the character of the medium,"[79] resulting in a "failure to properly balance the important issues of free speech, intellectual property rights, and criminal intent."[80] Although the law may have been intended to protect legitimate state interests, the result is constitutionally flawed and difficult to apply without severely handicapping the essential nature of the Internet.

In order to succeed at curtailing the crime that exists on the Internet, legislators must act with some sophistication rather than mere brute force. They must avoid prohibiting essential activities, and they must recognize that curtailing behavior on the Internet presents some constitutional issues as well. The Supreme Court has said that the Internet is a "unique and wholly new medium of worldwide human communication,"[81] and, moreover it is "the most participatory form of mass speech yet developed, [and] is entitled to the highest protection from governmental intrusion."[82] Any attempt to curtail speech on the Internet, therefore, will raise First Amendment issues and be subject to the strictest scrutiny by the courts. Additionally, because of the fundamental way the Internet is assembled, any state attempt to regulate it might affect users everywhere and might raise issues under the Commerce Clause, as well, unless such regulations are carefully drafted.[83]

In *Miller*, the court indicated that the Georgia legislation was overbroad. Successful and effective Internet legislation, therefore, needs to be narrowly tailored to address specific harmful conduct while not proscribing useful or protected conduct. The court also found it likely that the Georgia legislation was void for vagueness. Hence, new laws need to be clearly drafted so that the conduct they do proscribe will be readily apparent. Finally, any state legislation regulating the Internet needs to be written in such a way that it does not place undue burdens on users outside that state.

---

79. *Fraser*, *supra* note 33, at 243.

80. *Id.*

81. Reno v. American Civil Liberties Union, 521 U.S. 844, 117 S. Ct. 2329, 2334 (1997) (quoting American Civil Liberties Union v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996)).

82. 117 S. Ct. at 2340 (quotations omitted).

83. *See* American Libraries Assoc. v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).

BERKELEY TECHNOLOGY LAW JOURNAL
ANNUAL REVIEW OF LAW AND TECHNOLOGY

TELECOMMUNICATIONS