5 Va. J.L. & Tech. 3 (2000) <http://www.vjolt.net>
1522-1687 / © 2000 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL of LAW and TECHNOLOGY

UNIVERSITY OF VIRGINIA	SYMPOSIUM 2000	5 VA. J.L. & TECH. 3

The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity

David L. Sobel[*]

I. Introduction

1. Over the past few years, the Internet's popularity has increased dramatically. The ease with which online users can communicate with each other, view information, and conduct commercial transactions have been among the main attractions of the medium. Anonymity -- the ability to conceal one's identity while communicating -- has also been an appealing characteristic for a majority of Internet users. Individuals are able to post to message boards, converse in chatrooms, and visit informational sites while keeping their identities private. This anonymity allows the persecuted, the controversial, and the simply embarrassed to seek information -- and disseminate it -- while maintaining their privacy and reputations in both cyberspace and the material world.
2. Ironically, the anonymity that has contributed to the Internet's growing popularity is coming under attack. Armed with broad warrant and subpoena powers, law enforcement agencies are finding cyberspace to be fertile ground for the conduct of investigations, often seeking the identities of anonymous users.[1] Raising significant privacy concerns for the average Internet user, civil litigants increasingly are using the discovery process to pierce the veil of online anonymity. This article will address the individual's significant interest in anonymity, the growing challenge to this vital attribute of the Internet and possible procedural remedies to protect the identities of legitimate users.

II. Anonymity and Free Speech

3. While the personal privacy interest in controlling the disclosure of one's identity is apparent, anonymity also plays an important role in fostering free expression. The protection of anonymity thus takes on added significance on the Internet, a medium which provides individuals with unprecedented opportunities to both publish and receive information. While the expressive powers of the Internet have long been understood by its users, the medium's potential attained recognized constitutional status only in 1997. In ACLU v. Reno[2], the Supreme Court reviewed the Communications Decency Act[3], the first federal statute seeking to regulate Internet content. In a landmark decision defining the scope of the online medium's First Amendment protection, the Court noted that the Internet

   provides relatively unlimited, low-cost capacity for communication of all kinds . . . [t]his dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.[4]

4. The Court concluded that there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."[5]

5. What the Court described as "the vast democratic fora of the Internet"[6] would be stifled if users were unable to preserve their anonymity online. The courts have long recognized that compelled identification can chill expression. In McIntyre v. Ohio Elections Commission,[7] the Court struck down an Ohio statute prohibiting the anonymous distribution of campaign literature, noting:

   The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible.[8]

   Anonymity is a shield from the tyranny of the majority . . . It thus 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.[9]

6. It is clear that anonymity often facilitates free expression, particularly where controversial or unpopular ideas are being voiced.[10] Nondisclosure of identity is thus critical for websites, message boards and chat areas devoted to many topics, including corporate and governmental whistleblowing; labor organizing; dissident movements in repressive countries; gay and lesbian issues; and resources dealing with addiction, alcoholism, diseases and spousal abuse.[11]

III. The Challenges to Anonymity

A. Law Enforcement Access to User Identities

7. Citing the potential use of anonymity to conceal criminal activity, the Federal Bureau of Investigation has advocated the development and use of technical means to identify Internet users. For instance, FBI Director Louis Freeh told a Senate subcommittee in 1998 that identifying information such as Internet Working Protocol numbers, or "IP addresses,"[12] and Caller ID data should be captured and retained by Internet Service Providers. Such procedures, according to Freeh, would "greatly assist law enforcement in child pornography/child sexual exploitation investigations."[13]

8. One recent high-profile criminal case underscores the law enforcement interest in countering online anonymity, and the resulting privacy concerns. During its investigation of the Melissa e-mail virus, the FBI obtained information from America Online that led investigators to a telephone line in the home of computer programmer in New Jersey.[14] The programmer, David L. Smith, recently pleaded guilty to state and federal charges growing out of the incident.[15] Despite the successful apprehension of the virus writer, the FBI's investigative methods were criticized by members of a Congressional oversight committee on privacy grounds.[16]

9. Law enforcement access to information concerning Internet users is generally governed by the Electronic Communications Privacy Act ("ECPA").[17] The statute was enacted in 1986 to update federal wiretap law to better conform with then-new technologies like electronic mail. When law enforcement seeks access to the actual content of a communication -- such as the text of an e-mail message -- ECPA requires judicial issuance of a warrant under specified procedural requirements.[18] Defeating user anonymity is far less onerous for government investigators; disclosure of information identifying a particular user[19] is authorized upon presentation of an administrative subpoena to a service provider.[20]

B. Civil Discovery of User Identities

10. While ECPA's relatively liberal standard for law enforcement access to identifying information raises significant privacy concerns, greater controversy surrounds the state of the law governing non-governmental access to such data. The statute is written permissively and provides that a service provider "may disclose a record or other information pertaining to a subscriber . . . to any person other than a governmental entity." [21] With the explosive growth of the Internet, the lack of statutory protection for such information is creating a substantial challenge to personal privacy. Increasingly, criminal investigators are not the only ones seeking to pierce the veil of online anonymity. The civil court dockets are now seeing a growing number of cases in which the identities of anonymous Internet users are being sought. Typically, the cases are filed by corporations that have been the subjects of critical information posted to online message boards hosted at websites such as Yahoo! Finance, The Motley Fool, Raging Bull and Silicon Investor.
11. With the emergence of online trading,[22] financial message boards have become popular (and controversial) forums for the exchange of information on publicly traded companies.[23] In a recent speech, Commissioner Laura S. Unger of the Securities and Exchange Commission discussed the impact of the Internet on the investment world and noted that it can be a double-edged sword for companies:

    The same technology that lets companies communicate with investors also lets investors communicate with each other. The instrument of better investor relations can easily become the instrument by which investors challenge management, and it is no secret that investors are increasingly challenging management. . . .

12. Companies have to worry about chat rooms and bulletin boards because the Internet allows for rapid dissemination of information to a large audience. Disgruntled employees can easily post information anonymously which may move a company's stock price. Some short sellers are getting into the act as well by posting "cybersmears" about a company.[24]

13. With increasing frequency, "worried" companies are going to court. Since 1998, scores of civil lawsuits have been filed against "John Doe" defendants by plaintiffs allegedly harmed by anonymous Internet postings. [25] The underlying causes of action vary, ranging from defamation[26] to unauthorized disclosure of proprietary information.[27]

14. The common denominator in these suits is that they all raise novel yet fundamental questions of fairness and due process. Upon the filing of civil complaints, plaintiffs' counsel serve subpoenas on message board operators and Internet service providers seeking the identities of anonymous posters. Some service providers, including America Online, notify subscribers when civil subpoenas are received and allow them a period of time to challenge the process.[28] But many online services -- most notably Yahoo! -- comply with such subpoenas as a matter of course, without notice to their users.[29] As a result, "John Doe" defendants frequently have no opportunity to quash subpoenas and the courts have no role in evaluating the propriety of requests for identifying information. Indeed, there have been only a handful of known cases in which courts have heard motions to quash subpoenas served on Yahoo![30]

15. In the absence of adversarial proceedings to determine a plaintiff's entitlement to the identity of an anonymous Internet poster, the civil discovery process is open to potential abuse. The case of Raytheon Co. v. John Does 1-21[31] has been cited by several legal observers as an example of the problem. Alleging breach of contract and disclosure of proprietary information by company employees on a Yahoo! message board, Raytheon sued 21 "John Doe" defendants and subpoenaed Yahoo! for information identifying the individuals. After the company obtained the identities of the 21 defendants, it voluntarily dismissed its suit. [32] The dismissal raises questions concerning Raytheon's use of the discovery process: if (as the service of subpoenas would suggest) learning the identities of the Doe defendants was necessary for the adjudication of Raytheon's claims, why were those claims not litigated once the defendants were identified? The facts suggest that the company's sole objective was to unmask the anonymous posters, and that filing suit and obtaining subpoena power was the most expedient means of realizing that goal.

16. While there clearly will be cases in which aggrieved parties should be entitled to learn the identities of anonymous Internet posters, there will be many others in which the civil discovery process may be abused. Under current legal standards, lawsuits of questionable merit can be filed solely to obtain discovery and unmask anonymous speakers. Corporate critics can be chilled into silence, whistleblowers can be intimidated and gay people can be "outed."[33] Such a result would severely diminish the Internet's status as a democratic and vibrant marketplace of information and ideas.

17. The conflicts posed by online anonymity obviously require that a balance be struck between its benefits and potential abuse. From the perspective of constitutional values, it is clear that the balance should be weighted heavily toward the preservation of free and unfettered online expression. As the Supreme Court recognized in McIntyre, "[t]he right to remain anonymous may be abused when it shields fraudulent conduct. But . . . our society accords greater weight to the value of free speech than to the dangers of its misuse."[34]

IV. Leveling the Playing Field: Establishing Procedural Rights

18. The potentially conflicting interests in free expression and accountability must be balanced according to the facts and circumstances of a particular case. However, as noted, there is no existing mechanism for the adjudication of those interests: "John Doe" defendants are absent from the judicial process until their identities have been disclosed and the issue of anonymity has been mooted. Three proposed changes to current law would go a long way toward remedying that problem, ensuring procedural rights to anonymous Internet users when their identities are sought through civil discovery.

19. First, the Electronic Communications Privacy Act ("ECPA") should be amended to require the presentation of a subpoena before information identifying an Internet user can be disclosed to any party. As noted, the statute currently requires a subpoena only when a "governmental entity" seeks such information. A generally applicable subpoena requirement would be the first step toward ensuring due process rights for anonymous speakers.

20. Second, ECPA should require that upon receipt of a civil subpoena for information concerning a subscriber or user, a service provider must notify the individual of the request. A reasonable amount of time should be allowed for the individual to take appropriate action (i.e., move to quash) before any identifying information is disclosed. Currently, such rights of notification are provided, if at all, by service providers' Terms of Service or privacy policies. A uniform, federal right to notice would ensure that legitimate claims for the preservation of anonymity can be addressed by the courts.[35]

21. Finally, some measure of judicial oversight should be brought to the discovery process even when John Doe defendants are unable to retain counsel to defend their anonymity.[36] Congress and state legislatures should consider revisions to civil discovery procedures that would require a judge or magistrate to review subpoenas or other process seeking the identity of anonymous speakers when the anonymous defendant has not entered an appearance after receiving notice of the process. Such requirements should apply to cases involving speech-based claims against "John Doe" defendants to ensure that the underlying claims are legally valid and that discovery requests are not abusive or overly broad. The courts might also establish procedures whereby an anonymous defendant could submit pro se written objections to a subpoena without disclosing his or her identity to opposing counsel. Whatever the procedure, it is critical that some due process be brought to the unchecked, unilateral power to issue subpoenas and defeat anonymity.

V. Conclusion

22. Internet anonymity serves many legitimate ends but is subject to potential abuse. Despite the judicially-recognized benefits of anonymity, current law does not adequately protect the interests of individuals who choose to communicate on the Internet without disclosing their identities. In recognition of the important interests that Internet users have in the preservation of anonymity, legal protections should be established to provide a judicial framework and due process in the growing number of cases in which online anonymity is challenged.

Footnotes

[*] General Counsel, Electronic Privacy Information Center ("EPIC"), Washington, DC. The author gratefully acknowledges the assistance of EPIC law clerks Jason Abrams of Fordham University School of Law and Ethan Preston of the Georgetown University Law Center in the preparation of this article.

[1] The Circuit Court in Loudoun County, Virginia, the home of America Online, has been inundated with requests for warrants seeking information on AOL users. As of April 1999, 70 of the 107 applications filed with the court since the beginning of the year were directed to information maintained by the online service. Serving warrants on AOL is "almost a full-time job" for the Sheriff's investigator responsible for service. Stephen Dinan, *Search Warrants Keep AOL Busy*, WASHINGTON TIMES, April 27, 1999, at C4.

[2] Reno v. American Civil Liberties Union, 521 U.S. 844 (1997), *aff'g*, 929 F. Supp. 824 (E.D. Pa. 1996).

[3] The challenged provisions of the CDA were enacted as Title V of the Telecommunications Act of 1996, Pub.L.No. 104-104, §502, 110 Stat. 56, 133-35 (1996).

[4] 521 U.S. at 870.

[5] *Id*.

[6] *Id*. at 868.

[7] 514 U.S. 334 (1995).

[8] *Id*. at 341-42.

[9] *Id*. at 357. *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 a Georgia statute that would have made it a crime for Internet users to "falsely identify" themselves online).

Similarly, in Denver Area Educational Telecommunications Consortium, 518 U.S. 727 (1996), the Supreme 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 Reno v. ACLU, the Supreme Court found that the credit card and adult access code requirements of the CDA would also unconstitutionally inhibit adult Web browsers. 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.").

[10] The Court recognized in McIntyre the "respected tradition of anonymity in the advocacy of political causes" and noted that "even the arguments favoring the ratification of the Constitution advanced in the Federalist Papers were published under fictitious names." 514 U.S. at 342-43, *citing* Talley v. California, 362 U. S. 60, 64-65 (1960).

[11] *See, e.g.*, *The Importance of Anonymity* (visited Feb. 18, 2000) <http://www.alcoholics-anonymous.org/em24doc9.html>.

[12] Even where individuals have taken precautions, the Internet has a lowest common denominator of privacy: the IP address. It is not possible to connect to any computer on the Internet without using one. The IP address is typically recorded at both 1) the local server that provides the individual Internet access (typically called an Internet service provider or an ISP), which can relate it to the login name of the individual; and 2) a visited web site's server, which correlates that IP address' activities and the individual's activities on the website. "From an IP address, a server can determine the domain name . . . [and then] retrieve the name, physical location (e.g., country, state and zip code) and contact persons of the organization that originally registered that name . . ."

Although it is technically possible to forge an IP address by means of a proxy server or "spoofing," it is difficult and not necessarily within the average users' ability. Thus, knowledge of the IP address almost always leads to the organization which gave the targeted individual his or her Internet access. With the IP address and the time of the connection, "the ISP . . . will likely keep logs that identify the individual user, [along with] the remote computer contacted . . . and the date and time of contact."

Kang, *Information Privacy In Cyberspace Transactions*, 50 STAN. L. REV. 1193 at 1225, 1233 (1998). *See also* Lessig, *The Law of the Horse*, 113 HARV. L. REV. 501, 504-505 (1999).

[13] Louis J. Freeh , *Child Pornography on the Internet and the Sexual Exploitation of Children* (last modified March 10, 1998) <http://www.fbi.gov/pressrm/congress/congress98/sac310.htm>.

[14] Stephen Shankland, *Melissa Suspect Arrested in New Jersey* (last modified April 2, 1999) <http://news.cnet.com/news/0-1005-200-340689.html>. *See also* Joel Dean, *Melissa Manhunt Creates Precedent* (last modified April 7, 1999) <http://www.zdnet.co.uk/news/1999/13/ns-7648.html>.

[15] Erich Lvening, *Smith Pleads Guilty to Melissa Virus Charges* (last modified December 9, 1999) <http://news.cnet.com/news/0-1005-200-1489249.html>.

[16] *Congressman Questions FBI on Melissa Arrest* (last modified April 16, 1999) <http://www.zdnet.com/pcweek/stories/news/0,4153,1014408,00.htm>. Rep. David Wu (D-OR) was quoted as saying, "I believe in our society we are very concerned about privacy and anonymity and giving people space in which to act."

[17] 18 U.S.C. §§ 2510 et seq.

[18] 18 U.S.C. § 2518.

[19] Specifically, "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber to or customer of [an electronic communication] service and the types of services the subscriber or customer utilized." 18 U.S.C. § 2703(c)(1)(C).

[20] *Id*.

[21] 18 U.S.C. § 2703(c)(1)(A).

[22] In January 1999, Security and Exchange Commission Chairman Arthur Levitt stated that online trading accounted for approximately 25 percent of all retail stock trades and predicted that the number of online brokerage accounts would exceed 10 million by the end of the year. *Statement by Chairman Arthur Levitt Concerning On-Line Trading*, (last modified January 27, 1999) <http://www.sec.gov/news/press/99-9.txt>.

[23] Media Metrix, Inc. has reported that in June 1999 Yahoo! Finance attracted more than 5 million users; The Motley Fool logged 1.2 million; and Raging Bull and Silicon Investor each had a quarter million visitors. Kris Hundley, *Surfing the Message Boards* (last modified August 2, 1999) <http://www.sptimes.com/News/80299/Business/Surfing_the_message_b.shtml>.

[24] *Getting to Know You: Dealing with the Wired Investor, Remarks by Commissioner Laura S. Unger*, (last modified June 25, 1999) <http://www.sec.gov/news/speeches/spch287.htm>.

[25] While exact figures are impossible to ascertain, one report states that "[s]ince June 1988, American companies fighting . . . cyber-smears reportedly have been filing one or two lawsuits a week in Santa Clara County, Calif., the home of Yahoo! Inc." Blake A. Bell, *Dealing With the "Cybersmear,"* N.Y.L.J., April 19, 1999, at T3.

[26] *See, e.g., Lilly Files Message Board Defamation Suit* (last modified July 28, 1999) <http://news.cnet.com/news/0-1005-200-345458.html>.

[27] *See, e.g., Raytheon Sues 21 People Over Sharing of Company Secrets Online* (last modified March 5, 1999) <http://www.freedomforum.org/technology/1999/3/5raytheon.asp>.

[28] Tom Kirchofer, *Yahoo! Forum Case Raises Questions About Online Privacy* (last modified April 6, 1999) <http://detnews.com/1999/technology/9904/06/04060129.htm>. According to a company spokesman, "whenever AOL receives a subpoena in a civil case, it always notifies the member, giving the person 14 days to try to quash the subpoena." While the AOL Terms of Service do not obligate the company to notify subscribers upon receipt of civil subpoenas, it has been AOL's practice to do so.

[29] Representatives of Yahoo! have stated on several occasions that users are provided adequate notice through the company's policy statement on disclosure of personal information. Yahoo!'s privacy policy provides, in pertinent part:

Yahoo! may also disclose account information in special cases when we have reason to believe that disclosing this information is necessary to identify, contact or bring legal action against someone who may be violating Yahoo!'s Terms of Service or may be causing injury to or interference with (either intentionally or unintentionally) Yahoo!'s rights or property, other Yahoo! users, or anyone else that could be harmed by such activities. Yahoo! may disclose or access account information when we believe in good faith that the law requires it and for administrative and other purposes that we deem necessary to maintain, service, and improve our products and services.

Yahoo! Privacy Policy (visited Feb. 20, 2000) <http://docs.yahoo.com/info/privacy/>. Neither the privacy policy nor the company's practices provide user's with actual notice of pending subpoenas for personal information.

[30] *See, e.g.*, Xircom, Inc. v. John Doe, Case No. CIV 188724 (Superior Court of the State of California for the County of Ventura 1999). Without a written opinion, the court quashed the initial subpoena on procedural grounds but permitted Xircom to serve a second subpoena on Yahoo!. Rebecca Fairley Raney, *Judge Rejects Online Critic's Efforts to Remain Anonymous* (last modified June 15, 1999) <http://www.nytimes.com/library/tech/99/06/cyber/articles/15identity.html>. Prior to the re-issuance of the subpoena, the parties settled the lawsuit. Carl S. Kaplan, *Company Settles Suit Against Online Critic* (last modified July 16, 1999) <http://www.nytimes.com/library/tech/99/07/cyber/articles/16xircom.html>.

[31] Civil Action No. 99-816 (Commonwealth of Massachusetts Superior Court, Middlesex County, Filed February 1, 1999). The complaint is available online at <http://www.intelico.com/johndoe1.htm>.

[32] *Raytheon Drops Suit Over Internet Chat*, Associated Press (last modified May 22, 1999) <http://www.nytimes.com/library/tech/99/05/biztech/articles/22raytheon.html>.

[33] The "outing" of a gay Internet user was at issue in McVeigh v. Cohen, 983 F. Supp. 215, 219 (D. D.C. 1998). In apparent violation of both ECPA and its Terms of Service, America Online disclosed information to the U.S. Navy that identified an AOL subscriber (and sailor) as being gay. A resulting discharge proceeding against the sailor was enjoined by the district court, which observed that "enforcement of the ECPA is of great concern to those who bare the most personal information about their lives in private accounts through the Internet." *Id*. at 221.

[34] 514 U.S. 334, 357 (1995), *citing* Abrams v. United States, 250 U.S. 616, 630-31 (1919) (Holmes, J., dissenting).

[35] The type of inquiry that courts should make when assessing the merits of maintaining anonymity was described by the court in Columbia Insurance Co. v. SEESCANDY.com, 185 F.R.D. 573, 578 (N. D. Cal. 1999). The court noted that "the need to provide injured parties with a forum in which they may seek redress for grievances . . . must be balanced against the legitimate and valuable right to participate in online forums anonymously or pseudonymously." The court then articulated a four-part test for "the determination of whether discovery to uncover the identity of a defendant is warranted." *Id*.

First, the plaintiff should identify the missing party with sufficient specificity such that the Court can determine that defendant is a real person or entity who could be sued in federal court . . . This requirement is necessary to ensure that federal requirements of jurisdiction and justiciability are satisfied . . . Second, the party should identify all previous steps taken to locate the elusive defendant. This element is aimed at ensuring that plaintiffs make a good faith effort to comply with the requirements of service of process and specifically identifying defendants . . . Third, plaintiff should establish to the Court's satisfaction that plaintiff's suit against defendant could withstand a motion to dismiss. A conclusory pleading will never be sufficient to satisfy this element . . . Lastly, the plaintiff should file a request for discovery with the Court, along with a statement of reasons justifying the specific discovery requested as well as identification of a limited number of persons or entities on whom discovery process might be served and for which there is a reasonable likelihood that the discovery process will lead to identifying information about defendant that would make service of process possible.

Id. at 578-80.

[36] John Doe defendants do not have the option of appearing pro se for two reasons. First, a personal appearance would obviously negate a defendant's efforts to conceal his or her identity. Second, suits against John Does are frequently filed in jurisdictions distant to the defendants. As a result, anonymous defendants who wish to protect their identities are compelled to incur the expense of retaining counsel to represent them (assuming they are able to locate counsel in a distant jurisdiction on short notice).

Author Biography

David Sobel is general counsel of the Electronic Privacy Information Center (EPIC). He was formerly counsel to the National Security Archive (1986 - 1988) and an associate at Dobrovir, Oakes & Gebhardt (1983 - 1986), one of Washington's first public interest law firms. At EPIC, Mr. Sobel has litigated numerous cases under the FOIA seeking the disclosure of government information on cryptography, Internet and privacy policy. Among his recent cases are those involving the Digital Signature Standard, the Clipper Chip, the FBI's Digital Telephony proposal and the so-called 2600/Pentagon City Raid. He was co-counsel in Reno v. ACLU, the successful constitutional challenge to the Communications Decency Act decided by the U.S. Supreme Court in June 1997. Mr. Sobel served on the Association for Computing Machinery's Special Panel on Cryptography Policy, which produced the report Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy. He has written several articles concerning cryptography policy, including an article for the Computer Law Reporter titled "Governmental Restrictions on the Development and Dissemination of Cryptographic Technologies" (1993).

Discussion

Name: Lonnie Schooler Title: Attorney Affiliation: Jackson Walker	Presuming statutory protection of encrypted code is inadequate or unconstitutional, what do you suggest a developer of software for export require in a contract with a purchaser/importer to protect against code cracking or pirating of the software, or the products being purchased online?
Name: Richard W. Boone Jr. Title: Editor-in-Chief 2000-2001 Affiliation: Va J L & Tech	It seems as though there is a serious conflict here between interests of consumers and businesses in allowing the free export of encryption software and the interests of the U.S. government in preventing international distribution of this technology. Both consumers and businesses need the technology because it improves data security and thereby aids international commerce. However, the international distribution of high-powered encryption software implicates grave concerns both for national security officials and law enforcement because this technology greatly hinders intelligence gathering efforts. Providing "backdoor" access to encrypted information does not necessarily resolve this issue because it makes the data more vulnerable. Therefore, before any uniform encryption policy is developed, the U.S. government's concerns must be addressed.