REPORT OF THE
DEPARTMENT OF EDUCATION

Discovery of Electronic Data

TO THE GOVERNOR AND
THE GENERAL ASSEMBLY OF VIRGINIA

SENATE DOCUMENT NO. 9

COMMONWEALTH OF VIRGINIA
RICHMOND
2002

EXECUTIVE SECRETARY
ROBERT N. BALDWIN

ASST. EXECUTIVE SECRETARY
FREDERICK A. HODNETT, JR.

SUPREME COURT OF VIRGINIA
ADMINISTRATIVE OFFICE
THIRD FLOOR
100 NORTH NINTH STREET
RICHMOND, VIRGINIA 23219-2334
(804) 786-6455
FACSIMILE
(804) 786-4542

DIR., DISPUTE RESOLUTION SERVICES
GEETHA RAVINDRA
DIR., EDUCATIONAL SERVICES
THOMAS N. LANGHORNE, III
DIR., FISCAL SERVICES
JOHN B. RICKMAN
DIR., JUDICIAL PLANNING
KATHY L. MAYS
DIR., LEGAL RESEARCH
STEVEN L. DALLE MURA
DIR., MGMT. INFORMATION SYSTEMS
KENNETH L. MITTENDORFF
DIR., PERSONNEL
CATHERINE F. AGEE
DIR., TECHNICAL ASSISTANCE
DONALD R. LUCIDO

November 30, 2001

MEMORANDUM

TO: The Honorable James S. Gilmore III
Governor of Virginia

And

The General Assembly of Virginia

IN RE: Senate Joint Resolution No. 334

Pursuant to Senate Joint Resolution No. 334, I am pleased to submit this study on "The Discovery of Electronic Data".

Respectfully submitted

Robert N. Baldwin

Robert N. Baldwin
Executive Secretary

Preface

Introduction. This report responds to the directions of the General Assembly embodied in a study resolution during the 2001 Session (reprinted in Part I below) calling for an investigation into issues relating to the disclosure of the information maintained by electronic communications service providers in Virginia, particularly the legal procedure for subpoena of such information and the application of that procedure in cases where litigation pending outside the Commonwealth of Virginia results in an application to the Virginia courts for orders compelling disclosure of information. In practice, the most frequently litigated issue is the identity of persons communicating on the Internet anonymously.

This study is timely. Subpoenas seeking the identity of anonymous Internet posters are a substantial and growing phenomenon. In 2000, America Online received approximately 475 civil subpoenas, the vast majority of which sought identity information about its subscribers.[1] This represented an increase of almost 40% over the levels experienced even during the prior year.[2] This is also the experience in other states where large service providers are located. Since June 1998, approximately 2 subpoenas seeking an online identity have been filed *per week* in Santa Clara County, California, the jurisdiction in which the corporate headquarters of service provider "Yahoo!" are located.[3]

Some observers have suggested that the proliferation of lawsuits and subpoenas aimed at identifying Internet communicators threatens to have a chilling effect on protected speech and the growth of the online medium.[4] Although the use of legal processes to punish and deter truly tortious and harmful speech is appropriate, filing lawsuits simply as a pretext to compel the disclosure of a speaker's identity "threaten[s] not only to deter the individual who is sued from speaking out, but also to encourage undue self-censorship among the other John Does who frequent Internet discussion fora."[5] Indeed, "[a]s more and more suits are filed, many Internet users will come to recognize the ease with which their online anonymity can be stripped simply by the filing of a libel action, and they will censor themselves accordingly."[6] In view of this threat, it is incumbent upon the Commonwealth and its courts to apply a rigorous

---

[1] Brief Amicus Curiae of America Online, Inc. at 11, Melvin v. Doe, Nos. 2115 WDA 2000 and 2116 WDA 2000 (Pa. Super. Ct, 2000).

[2] Id.

[3] Blake A. Bell, Dealing with the Cybersmear, N.Y.L.J., Apr. 19, 1999 at T-3. And according to one transcribed court hearing in which Yahoo! argued a motion to quash a subpoena seeking identifying information concerning a message-board user, Yahoo! receives "thousands" of these subpoenas.

[4] Brief Amicus Curiae of America Online, Inc., Melvin v. Doe, Nos. 2115 WDA 2000 and 2116 WDA 2000 (Pa. Super. Ct, 2000). at 12. See Greg Miller, "John Doe" Suits Threaten Internet Users' Anonymity, L.A. Times, June 14, 1999, at A1 ("[T]he growing volume of these suits — and the subsequent dropping of them in some cases after identities have been disclosed — makes some experts fear that the legal process is being abused by organizations seeking only to 'out' online foes."). In February 1999, for example, Raytheon filed a John Doe suit for alleged wrongful disclosure of confidential information by pseudonymous speakers and subpoenaed the names of 21 individuals from Yahoo!. After Yahoo! supplied the names, Raytheon dropped the suit and fired four of the Does, who turned out to be Raytheon employees. Elinor Abreu, EPIC Blasts Yahoo for Identifying Posters, The Industry Standard, Nov. 10, 1999. At least some of the information claimed by Raytheon to have been unlawfully posted had in fact been disclosed one month earlier in public filings made by Raytheon itself. Ross Kerber, Raytheon Had Revealed "Secrets," Boston Globe, Apr. 9, 1999, at C1.

[5] Lyrissa B. Lidsky, Silencing John Doe: Defamation & Discourse in Cyberspace, 49 Duke L.J. 855, 861 (Feb. 2000).

[6] Id. at 889.

standard to ensure that "[p]eople who have committed no wrong [can] participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity." [7] Another key goal is to protect the service providers from undue harassment, and to provide a clear, simple and effective method for presenting the legal issues to the court in contested cases.

Table of Contents

The Report is organized as follows

[7] Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999).

Executive Summary

This Report sets forth the results of the Study conducted pursuant to the directions contained in Senate Joint Resolution 334, 2001 Session of the General Assembly. The Report first introduces the importance of the Internet and World-Wide Web as forums for communication protected by Constitutional free speech rights, as recognized by the United States Supreme Court and consistent with pre-existing Virginia law. The role of *anonymous speech* in this medium is discussed, along with federal and Virginia law relevant to an understanding of the importance that anonymity plays in the free expression of ideas, under protections for free expression, privacy and freedom of association with others.

The Report canvasses the existing case law directly on the topic of requests for confidential information relating to electronic communications, which is not extensive. Analogies from other, more developed, bodies of law are sketched. The prevailing standards for decisions on contested applications to pierce the anonymity of protected communications in civil litigation are discussed: the key to this analysis is that in order for a trial court to perform the *balancing of rights* necessary for a determination of whether intrusion upon protected anonymous speech will be allowed, the court must first be provided with the information it needs to perform that balancing. To decide these issues, the trial court in Virginia need not decide the *merits* of the case pending elsewhere, but must have sufficient considerations illuminated by the parties' submissions to permit assessment of the need for the contested information, on the one hand, and the severity of the intrusion on free speech, on the other. Tests applied in this situation by other courts, state and federal, are summarized and assessed in the Report.

A brief summary of how the subpoena process now operates in the federal courts and the Virginia circuit courts is provided in the body of the Report, along with several analogous procedures and doctrines that suggest considerations for inclusion in any effort to provide a unified approach to subpoenas for electronic information.

The relevant considerations and factors are specifically set forth and discussed, and a proposed statute or rule embodying the applicable provisions is then proposed. The procedure discussed involves six steps:

❶ **Initiation of the Subpoena.** The applicant for a subpoena seeking information calculated to identify a person communicating anonymously on the Internet or World-Wide Web, must provide to the court in Virginia (either in obtaining a court-issued subpoena or by filing immediately after promulgating an attorney-issued subpoena) *at least 30 days prior to the scheduled disclosure*, a subpoena package containing the text of the subpoena itself, along with supporting information showing (i) that one or more

communications that are or may be tortious or illegal have been made by the anonymous person, or that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed, (ii) that other efforts to identify the anonymous communicator have proven fruitless, (iii) that the identity of the anonymous communicator is important, i.e., is centrally needed to advance the claim, relates to a core claim or defense, or is directly and materially relevant to that claim or defense, (iv) that the actionability of the communications cannot be determined while the author remains anonymous (i.e. that no motion to dismiss, motion for judgment on the pleadings, or judgment as a matter of law, demurrer or summary judgment-type motion challenging the viability of the lawsuit of the underlying plaintiff, is pending), and (v) that the persons or entities to whom the subpoena is addressed are likely to have responsive information. The applicant serves two copies of these papers upon the subpoenaed party, along with payment sufficient to cover postage for remailing of one copy of the application within the United States, registered and with return receipt.

❷ **Transmission to the Anonymous Communicator.** Within five business days after receipt of a subpoena application calling for identifying information concerning a client, subscriber or customer, the subpoenaed party mails one copy thereof, by registered mail or commercial delivery service, return receipt requested, to the client, subscriber or customer whose identifying information is the subject of the subpoena.

❸ **Time for Objection or Motion**. At least five business days prior to the date on which disclosure is sought under the subpoena, any interested person may file a detailed written objection, motion to quash, or motion for protective order, which may set forth all grounds for opposing the disclosure sought in the subpoena, and must address to the extent feasible (i) whether the identity of the anonymous communicator has been disclosed in any fashion, (ii) whether the subpoena fails to allow a reasonable time for compliance, (iii) whether it requires disclosure of privileged or other protected matter and no exception or waiver applies, or (iv) whether it subjects a person to undue burden.

❹ **Timing of Compliance With Subpoena.** The party to whom the subpoena is addressed may not comply with the subpoena earlier than three business days before the date on which disclosure is due, to allow the anonymous client, customer or subscriber the opportunity to object.

❺ **Stay of Compliance Pending Court Action**. If any person files an objection, motion to quash, or motion for protective order, compliance with the subpoena shall be deferred until the appropriate court rules on the obligation to comply.

The Report discusses the operation of these steps, and the draft enactment contains significantly greater detail and more precise language than the summary above.

Conclusion. The Report's Conclusion is that the significance of Internet communications, and the constitutional protections that guard these communications suggest

that legislative guidance and implementation of a careful procedure appear highly desirable. The national trend toward increased litigation about anonymous communications imposes repeated burdens on trial courts, and litigation pending in another jurisdiction adds even further layers of complexity to constitutional doctrine, which requires a delicate weighing of competing values. The fact that the anonymous communicators are often laypersons with little access to legal representation complicates the picture still further. Present day subpoena practice does not assure the interested parties sufficient time or procedural protections and fails to equip the courts with information needed to decide disputed applications. Properly crafted rules would assure:

(A) that the Commonwealth's citizens have the full protections the Virginia and federal Constitutions provide to them, and an appropriate and fair opportunity to protect those rights; and

(B) that enterprises who possess identifying information be protected from unnecessary entanglement with litigations, and are compelled to make disclosure only when proper standards have been met; and

(C) that the Commonwealth's judges are provided with the information they need for full and fair consideration of the relevant factors in ruling on such disputes.

Hence codification of the rights and procedures involved is recommended.

Appendices are annexed to the Report, sketching related issues that are not dealt with comprehensively in the body of this submission, summarizing the most complete Supreme Court of Virginia decision dealing with this topic, and setting forth a bibliography of relevant literature.

I

STUDY RESOLUTION DEFINES AREAS FOR REPORT

The General Assembly passed Senate Joint Resolution 334 on February 22, 2001, which provides for a study of the discovery of electronic data and proposal of a statutory scheme or rules of evidence to govern the discovery of electronic data in civil cases in the courts of Virginia.

The text of the Study Resolution is as follows:

WHEREAS, Virginia is the center of the Internet, with numerous multi-state and multi-national Internet businesses located in the Commonwealth; and

WHEREAS, numerous motions regarding the discovery of electronic data are being heard in the circuit courts of the Commonwealth; and

WHEREAS, many of these motions arise out of cases pending in other states but are being heard in the Commonwealth solely because the Internet service providers (ISPs), which may be the custodians of such electronic data, are located in the Commonwealth; and

WHEREAS, the Code of Virginia provides a statutory scheme for governing the discovery of such electronic data for criminal cases but not for civil cases; and

WHEREAS, to strengthen the Commonwealth's position as the leader of technology and relevant laws and to facilitate further growth of Internet industries, a legal procedure governing the discovery of electronic data, whether by statute or by rules of evidence, is necessary; now, therefore, be it

RESOLVED by the Senate, the House of Delegates concurring, That the Office of the Executive Secretary of the Virginia Supreme Court, in consultation with the Joint Commission on Technology and Science, be requested to study the discovery of electronic data. The Executive Secretary shall examine the development of a statutory scheme or rules of evidence to govern the discovery of electronic data in civil cases and the feasibility of providing circuit court judges the authority to appoint special commissioners to hear and resolve complex disputes regarding the discovery of electronic data.

All agencies of the Commonwealth shall provide assistance to the Executive Secretary, upon request.

The Office of the Executive Secretary of the Virginia Supreme Court shall complete its work in time to submit its findings and recommendations by November 30, 2001, to the Governor and the 2002 Session of the General Assembly as provided in the procedures

of the Division of Legislative Automated Systems for the processing of legislative documents.[8]

The Resolution obviously reflects a need for guidance for Virginia courts when they are required to evaluate requests for electronic information. Of particular concern are discovery requests for identifying information on anonymous Internet users. Complex conflicts of interest are inherent in such requests, and the interests and rights of all parties involved must be carefully considered and weighed. Virginia courts require guidance in balancing these interests to ensure consistent and appropriate results.

Anonymous Remailing Distinguished. Services exist by which a person wishing to remain anonymous can route his or her communications through an "anonymous remailer", which is a computer operation that strips identifying information out of the communication and sends it along to the intended recipients without any traceable record of who actually sent it. Both legal and illegal communications have on occasion been transmitted in this fashion, and certain foreign locales have acquired dubious notoriety because of anonymous remailing operations conducted on their soil. No indication has been received to suggest that any providers of this sort of service are headquartered in Virginia. The topic of this Report is the more normal sort of anonymity in electronic communications, in which a subscriber uses a moniker other than his or her real name under a subscription agreement with an Internet service provider, which maintains records that would allow the authorities, and a private party successful in enforcing a subpoena, to learn the person's identity. Some writers have proposed that legal standards should be set for the length of time that a service provider should maintain records of users' names and addresses, to facilitate production of information under properly approved subpoenas.[9] Since there is no indication to date of improper record keeping by Virginia service providers, no proposals are advanced in this Report in this connection.

Report Preparation. The Office of the Executive Secretary of the Supreme Court directed preparation of this Report to address the matters raised in the Study Resolution. During May – December, 2001, extensive research into the issues identified by the General Assembly was undertaken.

Early in the process the two Virginia circuit court judges who have fielded the majority of litigation in this subject area were contacted. In addition to oral interviews with Judge Thomas D. Horne, and written submissions to the study files from both Judge Horne and Judge Stanley P. Klein, telephone interviews were conducted with Laura A. Heymann, Esquire of Counsel, America Online, Inc., Clerks Staff, Loudoun County Circuit Court, and Professor Lyrissa Lidsky, University of Florida College of Law. Information was solicited and received

---

[8] 2001 VA S.J.R. 334 (2001).

[9] See, e.g., Suman Mirmira, Annual Review of Law and Technology: Business Law, Lunney v. Prodigy Services Co., 15 Berkeley Tech. L.J. 437 (2000) (mandatory record-keeping solves the problem of accountability, provides a way for an injured party to be made whole by a defaming party, and deters individuals from posting defamatory messages because they would be identifiable under subpoena). Compare: Noah Levine, Note: Establishing Legal Accountability for Anonymous Comunication in Cyberspace, 96 Colum. L. Rev. 1526 (October 1996) (mandatory record-keeping allowing for identification of senders of specific messages is comparable to existing statutes requiring maintenance of certain business records, with civil penalties for failure to comply).

from Megan Gray, Esquire, Baker & Hostetler, L.L.P., Paul Alan Levy, Public Citizen Litigation Group, and Justin Allen, Esquire, Wright, Lindsey & Jennings.

Drafts of this Report were circulated for comment to numerous of the above-listed persons, as well as to Josh Levi, Director of Policy, Northern Virginia Technology Council, and to personnel in the Office of the Executive Secretary of the Supreme Court of Virginia.

Extensive searches were made of the legal periodicals and other sources dealing with Internet communications, freedoms of speech and assembly, defamation, privacy, and other topics. A bibliography of relevant literature is set forth as Appendix C of this Report.

This Report was prepared by the Project Reporter, Professor Kent Sinclair, University of Virginia School of Law.[10]

[10] Professor Sinclair expresses his appreciation to Mary L. McGinnis, University of Virginia School of Law, for research assistance in connection with the drafting of this Report, and to Robert N. Baldwin, Executive Secretary of the Supreme Court of Virginia, for guidance throughout the project.

II

THE INTERNET AND WORLD-WIDE WEB ARE RECOGNIZED AS IMPORTANT FORUMS FOR COMMUNICATION PROTECTED BY CONSTITUTIONAL FREE SPEECH RIGHTS

Strong Protection for Internet Speech. The United States Supreme Court has found that the Internet is "the most participatory form of mass speech yet developed," and is entitled to "the highest protection from governmental intrusion."[11] Content of speech is so vigorously protected in this context because of the Internet's unique nature as a communication forum: (1) it presents very low barriers to entry, (2) ease of use is identical for both communicators and observers, (3) as a result, astoundingly diverse content is available in this forum, and (4) the Internet provides significant access to all who wish to speak in the medium, and even creates a relative parity among speakers.[12] The Internet thus provides all citizens with unprecedented availability of unlimited, low-cost communication of all kinds, serving fundamental values of free expression:

> This 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 . . . [C]ontent on the Internet is as diverse as human thought.

In light of the special attributes of Internet communication, the Supreme Court held that the First Amendment[13] denies Congress the power to regulate the content of protected speech on the Internet.[14] The States are similarly precluded.[15]

Background and Development. The Internet is a "decentralized, global medium of communication that links people, institutions, corporations and governments around the world. It is a giant computer network that interconnects innumerable smaller groups of linked computer networks and individual computers. While estimates are difficult due to its constant and rapid growth, the Internet is currently believed to connect more than 159 countries and over

---

[11] ACLU v. Reno, 521 U.S. 844, 863 (1997).

[12] Id.

[13] Virginia Constitutional protections for the forms of speech involved in the present study are at least as great, and perhaps broader, than those of the federal First Amendment. See Part IV of this Report.

[14] ACLU v. Reno, 521 U.S. at 863.

[15] All fundamental rights comprised within the term liberty are protected by the Federal Constitution from invasion by the States. McIntyre v. Ohio Elections Commission, 514 U.S. 334, 336 (1995). The right of free speech, the right to teach and the right of assembly are, of course, fundamental rights. Id. See generally Marchioro v. Chaney, 442 U.S. 191, 193 n.2 (1979): "The freedom protected against federal encroachment by the First Amendment is entitled under the Fourteenth Amendment to the same protection from infringement by the States" (citing Williams v. Rhodes, 393 U.S. 23, 30-31 (1968).

137 million users."[16] The U.S. Supreme Court has outlined the history of the development of the Internet:[17]

> The Internet is an international network of interconnected computers. It is the outgrowth of what began in 1969 as a military program called "ARPANET," [Advanced Research Project Agency Network] which was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is "a unique and wholly new medium of worldwide human communication."
>
> The Internet has experienced "extraordinary growth." The number of "host" computers--those that store information and relay communications--increased from about 300 in 1981 to approximately 9,400,000 by the time of the trial in 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet at the time of trial, a number that is expected to mushroom to 200 million by 1999.
>
> Individuals can obtain access to the Internet from many different sources, generally hosts themselves or entities with a host affiliation. Most colleges and universities provide access for their students and faculty; many corporations provide their employees with access through an office network; many communities and local libraries provide free access; and an increasing number of storefront "computer coffee shops" provide access for a small hourly fee. Several major national "online services" such as America Online, CompuServe, the Microsoft Network, and Prodigy offer access to their own extensive proprietary networks as well as a link to the much larger resources of the Internet. These commercial online services had almost 12 million individual subscribers at the time of trial.
>
> Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e-mail"), automatic mailing list services ("mail exploders," sometimes referred to as "listservs"), "newsgroups," "chat rooms," and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium--known to its users as "cyberspace"--located in no

---

[16] Estimates for these figures were stipulated to by the State of New Mexico and the ACLU, and adopted by the federal court of appeals in a recent 10th Circuit case, ACLU v. Johnson, 194 F.3d 1139, 1153 (10th Cir. 2000). See n. 19 where the Department of Commerce estimated 137 million users as of 2000.

[17] See Reno v. ACLU, 521 U.S. 844, 849-57 (1997); Cyberspace, Communications, Inc. v. Engler, 55 F. Supp. 2d 737, 740-44 (E.D. Mich. 1999); American Libraries Assoc. v. Pataki, 969 F. Supp. 160, 164-67 (S.D.N.Y. 1997); Shea v. Reno, 930 F. Supp. 916, 925-34 (S.D.N.Y. 1996).

particular geographical location but available to anyone, anywhere in the world, with access to the Internet.

E-mail enables an individual to send an electronic message--generally akin to a note or letter--to another individual or to a group of addressees. The message is generally stored electronically, sometimes waiting for the recipient to check her "mailbox" and sometimes making its receipt known through some type of prompt. A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers. Newsgroups also serve groups of regular participants, but these postings may be read by others as well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic running the gamut from, say, the music of Wagner to Balkan politics to AIDS prevention to the Chicago Bulls. About 100,000 new messages are posted every day. In most newsgroups, postings are automatically purged at regular intervals. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real-time dialogue--in other words, by typing messages to one another that appear almost immediately on the others' computer screens. The District Court found that at any given time "tens of thousands of users are engaging in conversations on a huge range of subjects." It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought."

The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers, as well as, in some cases, to communicate back to designated sites. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. Some of these documents are simply files containing information. However, more elaborate documents, commonly known as Web "pages," are also prevalent. Each has its own address--"rather like a telephone number." Web pages frequently contain information and sometimes allow the viewer to communicate with the page's (or "site's") author. They generally also contain "links" to other documents created by that site's author or to other (generally) related sites. Typically, the links are either blue or underlined text--sometimes images.

Navigating the Web is relatively straightforward. A user may either type the address of a known page or enter one or more keywords into a commercial "search engine" in an effort to locate sites on a subject of interest. A particular Web page may contain the information sought by the "surfer," or, through its links, it may be an avenue to other documents located anywhere on the Internet. Users generally explore a given Web page, or move to another, by clicking a computer "mouse" on one of the page's icons or links. Access to most Web pages is freely available, but some allow access only to those who have purchased the right from a commercial provider. The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

From the publishers' point of view, it constitutes a vast platform from which to address and hear from a world-wide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers include government agencies, educational institutions, commercial entities, advocacy groups, and individuals. Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web."

"Web publishing is simple enough that thousands of individual users and small community organizations are using the Web to publish their own personal 'home pages,' the equivalent of individualized newsletters about the person or organization, which are available to everyone on the Web."[18]

The number of Internet users has continued to grow, increasing from 90,000 in 1993, to 137 million in the year 2000.[19] In the same timeframe, the number of U.S. households online rose from 6% to 42%.[20] Some observers predict that by the year 2003, 62% of Americans will be online, and that by the year 2005, 91% will be online.[21] This tremendous growth has created unprecedented opportunities for communication, but has also generated new legal challenges associated with the alleged abuse of those opportunities.

[18] ACLU v. Reno, 521 U.S. at 850-53, quoting findings made by the United States District Court for the Eastern District of Pennsylvania, at 929 F.Supp. 824, 837 (1996).
[19] U.S. Department of Commerce, Leadership for the New Millennium: Delivering on Digital Progress and Prosperity, The U.S. Government Working Group on Electronic Commerce, 3rd Annual Report, 2000, at http://www.ecommerce.gov/ecomnews/ecommerce2000annual.pdf.
[20] Id.
[21] Id.

III

ANONYMITY OF A COMMUNICATOR – WHILE POTENTIALLY DEFEASIBLE IN INSTANCES OF TORTIOUS OR CRIMINAL BEHAVIOR – IS A VALUE GIVEN STRONG CONSTITUTIONAL PROTECTION

Anonymous Speech. The right to speak anonymously, while not absolute, is broadly protected under the First Amendment.[22] The United States Supreme Court has held that the right of a speaker or writer to publish statements anonymously is a fundamental part of the right of free expression. Only the presence of compelling interests outweighing the need to preserve this aspect of freedom of expression will justify enforced disclosure of the identity of the author.[23]

Thus, in a landmark case, an ordinance prohibiting anonymous handbills was found to be an unconstitutional abridgment of the freedom of expression, because the identification requirement restricted the freedom to distribute information and thereby impinged upon freedom of expression.[24]

The historical importance of the right to communicate anonymously is clear. "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. . . . Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. . . . Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes."[25] The Court has also recognized the importance to First Amendment values of the right to *receive* information anonymously.[26]

The Supreme Court has considered the government's interest in identifying those responsible for fraud, false advertising or libel, but found that such goals did not vindicate the particular ordinance under review, since the law's provisions were not so limited, but barred all handbills, thereby restricting an individual's freedom to speak anonymously.[27]

The Supreme Court also observed that, in some circumstances, groups must be free to criticize oppressive practices anonymously or there will be no viable option to criticize at all.[28] In weighing governmental versus individual interests, the Court acknowledged a special need to preserve anonymity in this type of political speech.[29]

---

[22] Talley v. California, 362 U.S. 60, 65 (1960).
[23] Id. See also, e.g., Buckley v. Valeo, 424 U.S. 1 (1976); McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995).
[24] Talley, 362 U.S. at 64.
[25] Talley, 362 U.S. at 64-65.
[26] Lamont v. Postmaster General, 381 U.S. 301, 307 (1965).
[27] Talley, 362 U.S. at 63
[28] Id. at 64.
[29] Id. at 65.

Subsequently, the Supreme Court has recognized First Amendment protection for a communicator's anonymity *without any required showing of threats or possible reprisals.*[30] In reviewing laws requiring disclosure of campaign contributions, the Court noted that "compelled disclosure, in itself, can seriously infringe on privacy of association and belief guaranteed by the First Amendment."[31] Compelled disclosures of otherwise private speech acts were held to be a "significant encroachments on First Amendment rights."[32] In the context of compelled disclosure *pursuant to legislation*, the Court held that such encroachments on protected information "cannot be justified by a mere showing of some legitimate governmental interest . . . [W]e have required that the subordinating interests of the State must survive *exacting scrutiny.*"[33] The Court noted that there must be a "relevant correlation" or "substantial relation" between the governmental interest and the information required to be disclosed,[34] and that burdens on individual rights must be weighed carefully against the interests to be promoted by legislation.[35]

Strict scrutiny of the governmental justification for compelled disclosure is held necessary "even if any deterrent effect on the exercise of First Amendment rights arises, not through direct government action, but indirectly as an unintended but inevitable result of the government's conduct in requiring disclosure."[36] The need for this high level of justification is that "compelled disclosure has the potential for substantially infringing the exercise of First Amendment rights."[37]

More recently, the Court held that an author's right to communicate anonymously is protected under the First Amendment *whatever the reason for desiring anonymity may be*:

> [A]n author is generally free to decide whether or not to disclose his or her true identity. 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. Whatever the motivation may be, . . . the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[38]

---

[30] Buckley v. Valeo, 424 U.S. 1 (1976).
[31] Id. at 64, citing Gibson v. Florida Legislative Comm., 372 U.S. 539 (1963); NAACP v. Button, 371 U.S. 415 (1963); Shelton v. Tucker, 364 U.S. 479 (1960); Bates v. Little Rock, 361 U.S. 516 (1960); NAACP v. Alabama, 357 U.S. 449 (1958).
[32] Buckley, 424 U.S. at 64.
[33] Id. (emphasis added).
[34] Id., citing Bates v. Little Rock, 361 U.S. at 525; Gibson v. Florida Legislative Comm., 372 U.S. at 546.
[35] Id. at 68.
[36] Id. at 65.
[37] Id. at 66.
[38] McIntyre v. Ohio Elections Commission, 514 U.S. 334, 341-42 (1995). Accord: Buckley v. American Const. Law Found., 525 U.S. 182, 197-200 (1999)("name identification" required for political canvassers "without sufficient cause" was improper).

Application to Private Civil Litigation? The landmark decisions discussed above all involved the invalidation of broad statutes requiring disclosure. None involved a private tort litigant seeking to learn the identity of an anonymous speaker who allegedly has committed defamation, theft of trade secrets, or other actionable conduct. Thus, while the black letter-rule is clear that there is a presumption *ab initio* that the identity of an anonymous speaker is protected, recourse to case law developed in analogous situations is necessary in order to translate the "strict scrutiny" test (applicable to statutes and ordinances) to the context of identification demands in private civil tort litigation.

Before turning to discussion of that body of case law, it is worth noting that protection for anonymous communication under First Amendment and privacy doctrines are buttressed by further constitutional case law on the doctrine of freedom of association, as reflected in a series of seminal United States Supreme Court decisions.

Freedom of Association. Internet bulletin boards and discussion groups provide opportunities for posters to find and communicate with like-minded individuals, essentially creating "assemblies" of people who openly communicate on innumerable topics and issues. As a result, freedom of association principles are also pertinent to the present context. While detailed analysis of this area of law is available elsewhere,[39] the core doctrine can be sketched in short compass here.

The United States Supreme Court has held that the right of individuals to "associate" with other persons is a fundamental liberty protected under the First and Fourteenth Amendments from governmental intrusion.[40] While the freedom of association is not explicitly set out in the First Amendment, it has long been held to be implicit in the freedoms of speech, assembly, and petition.[41]

> "[I]mplicit in the right to engage in activities protected by the First Amendment" is "a corresponding right to associate with others in pursuit of a wide variety of political, social, economic, educational, religious, and cultural ends." This right is crucial in preventing the majority from imposing its views on groups that would rather express other, perhaps unpopular, ideas.[42]

The Court's decisions involving associational protections establish that the right of association is a "basic constitutional freedom,"[43] that is "closely allied to freedom of speech and a right

---

[39] The seminal work is Thomas I Emerson, Freedom of Association and Freedom of Expression, 74 Yale L.J. 1, 26 (1964). See also Donald T. Kramer, Annotation, The Supreme Court and the First Amendment Right of Association, 33 L. Ed. 2d 865 (1973).

[40] See, e.g., Boy Scouts of America v. Dale, 530 U.S. 640, 647 (2000), citing Roberts v. United States Jaycees, 468 U.S. 609, 622 (1984); NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 460-461 (1958). See also Runyon v. McCrary, 427 U.S. 160, 175-176 (1976) ("The Court has recognized a First Amendment right 'to engage in association for the advancement of beliefs and ideas").

[41] See, e. g., Baird v. State Bar of Arizona, 401 U.S. 1, 6 (1971); NAACP v. Button, 371 U.S. 415, 430 (1963); Louisiana v. NAACP, 366 U.S. 293, 296 (1961); NAACP v. Alabama, 357 U.S. 449 (1958) (Harlan, J., for a unanimous Court).

[42] Boy Scouts of America v. Dale, 530 U.S. 640, 647 (2000).

[43] Kusper v. Pontikes, 414 U.S. 51, 57 (1973).

which, like free speech, lies at the foundation of a free society."[44] The First Amendment protects freedom of association because it makes the right to express one's views meaningful.[45]

The Court has acknowledged the importance of freedom of association in guaranteeing the right of people to make their voices heard on public issues:

> Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly.[46]

Indeed, "inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."[47]

Of particular relevance to an "expressive" medium such as Internet communications, the Court has held "protection of the right to expressive association is 'especially important in preserving political and cultural diversity and in shielding dissident expression from suppression by the majority'."[48] Informal discussion groups are treated as expressive association for constitutional purposes.[49]

The Court has recently held that the freedom of expressive association is infringed where government compulsion "affects in a significant way the group's ability to advocate public or private viewpoints."[50]

Further, the ***anonymity*** of memberships and similar associational links is protected by the Constitution. The Court has held, for example, that in order to force the production of membership lists, the government's interest must be compelling.[51] Thus, in general, the right to associate freely includes the right to maintain anonymity in those associations.[52]

While the Supreme Court has not endorsed a limitless "right to individual anonymity [derived from the] freedom of association cases" it has emphasized that the anonymity protections implicit in those cases were necessary to protect "freedom of association for the

---

[44] Shelton v. Tucker, 364 U.S. 479, 486 (1960).
[45] See Board of Dirs. of Rotary Int'l v. Rotary Club of Duarte, 481 U.S. 537, 548 (1987), citing NAACP v. Claiborne Hardware Co., 458 U.S. 886, 907-908 (1982); Citizens Against Rent Control v. Berkeley, 454 U.S. 290, 295-299 (1981).
[46] NAACP v. Alabama, 357 U.S. at 460.
[47] NAACP v. Alabama, 357 U.S., at 462; NAACP v. Button, 371 U.S. 415. Accord: Brown v. Socialist Workers '74 Campaign Committee, 459 U.S. 87, 91(1982).
[48] Boy Scouts of America, 530 U.S. at 647, quoting Roberts, 468 U.S. at 622.
[49] "The First Amendment's protection of expressive association is not reserved for advocacy groups. But to come within its ambit, a group must engage in some form of expression, whether it be public or private." Boy Scouts of America, 530 U.S. at 648.
[50] 530 U.S. at 648.
[51] NAACP v. Alabama, 357 U.S. 449, 463 (1958).
[52] Id. at 466.

purpose of advancing ideas and airing grievances."[53] Compelled disclosure of a person's identity, associations or beliefs "can seriously infringe on privacy of association and belief guaranteed by the First Amendment."[54]

The freedom of expressive association, like many freedoms, is not absolute. The Court has held that its protections may be overridden "by regulations adopted to serve compelling state interests, unrelated to the suppression of ideas, that cannot be achieved through means significantly less restrictive of associational freedoms."[55] Thus, as in other free speech contexts, measures infringing on associational rights must be the least restrictive means to obtain the goal.[56]

Disclosure of the identity of a person associating in the discussion of ideas may yield on appropriate showings to the vindication of the rights of others. In another context the Court held that the "freedom of association protected by the First Amendment does not extend to joining with others for the purpose of depriving third parties of their lawful rights."[57]

---

[53] Whalen v. Roe, 429 U.S. 589, 603 n.32 (1977), citing Bates v. Little Rock, 361 U.S. at 522-23, NAACP v. Alabama, 357 U.S. at 462.

[54] Brown v. Socialist Workers '74 Campaign Committee, 459 U.S. 87, 91(1982), citing Buckley v. Valeo, 424 U.S. at 64, Gibson v. Florida Legislative Comm., 372 U.S. 539 (1963); NAACP v. Button, 371 U.S. 415 (1963); Shelton v. Tucker, 364 U.S. 479 (1960); Bates v. Little Rock, 361 U.S. 516 (1960); NAACP v. Alabama, 357 U.S. 449 (1958).

[55] 530 U.S. at 648, relying on Roberts at 623.

[56] Elrod v. Burns, 427 U.S. 347, 363 (1976) (government means must be "least restrictive of freedom of belief and association"); Kusper v. Pontikes, 414 U.S. 51, 58-59 (1973) ("[Even] when pursuing a legitimate interest, a State may not choose means that unnecessarily restrict constitutionally protected liberty").

[57] Madsen v. Women's Health Center, 512 U.S. 753, 776 (1994).

IV

UNDER VIRGINIA LAW, PROTECTION FOR ANONYMOUS COMMUNICATION IS AS GREAT, OR GREATER, THAN THAT PROVIDED BY THE FEDERAL CONSTITUTION

Freedom of Speech. Section 12 of the Virginia Bill of Rights may offer even greater protection for freedom of speech than does the First Amendment to the federal Constitution.[58] While there is no Virginia case law expressly delineating the margins of the right to communicate anonymously, protection for dissemination of oral and written speech are as strong or stronger under Virginia law than those provided by the First Amendment. Hence there is no reason to think that the protections for anonymous speech are any less vigorous in Virginia.

The language of § 12 of the Virginia Bill of Rights is more protective than that of the First Amendment. The Virginia Constitution, in Article I, § 12 states flatly – and expansively -- "[t]hat the freedoms of speech and of the press are among the great bulwarks of liberty, and can never be restrained except by despotic governments; that any citizen may freely speak, write, and publish his sentiments on all subjects, being responsible for the abuse of that right; that the General Assembly shall not pass any law abridging the freedom of speech or of the press, nor the right of the people peaceably to assemble, and to petition the government for the redress of grievances." This charter of speech rights has arguably greater reach than that set forth in the First Amendment:

> The Constitution of Virginia is broader that that of the United States in providing that – "any citizen may freely speak, write and publish his sentiments on all subjects." In Webster's New International Dictionary (2d Ed.), the word "publish" is defined as meaning: "to bring before the public as for sale or distribution."[59]

Thus there may be greater protections for speech interests under Virginia Constitutional principles, applicable directly in the context of concern here: the focus on a right to "publish" guarantees Virginians the right to "distribute" ideas in various channels of communication, such as the electronic forums of interest in the present study.

Association Rights in Virginia. As noted above, Article I, § 12 of the Constitution of Virginia provides "that the General Assembly shall not pass any law abridging . . . the right of the people peaceably to assemble. . ." Even before the addition of this explicit language in 1969, the Virginia courts had recognized the right peaceably to assemble. [60]

Like the federal Constitution, no express statement of association rights is included in the Virginia Constitution beyond this reference to the right to "assemble." The Commission on Constitutional Revision received a proposal that the Bill of Rights include a guarantee of freedom of association, but thought it "wiser to leave it to the courts to decide, in the context of

---

[58] Robert v. City of Norfolk, 188 Va. 413, 420, 49 S.E.2d 697, 732 (1948).
[59] Robert, 188 Va. at 420, 49 S.E.2d at 732.
[60] York v. City of Danville, 207 Va. 665, 152 S.E.2d 259 (1967), noted in 53 Va. L. Rev. 1567 (1967).

concrete cases, to what extent a right of association is implicit in other constitutional rights and how that right is to be applied to specific factual situations."[61]

Adopting language of the United States Supreme Court, the Supreme Court of Virginia has held: "It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment which embraces freedom of speech."[62] Thus there is well recognized in Virginia a "constitutionally protected right of freedom and privacy of association".[63] The Virginia Supreme Court went on to espouse the view that non-disclosure of a person's identity as a participant in a group associated with various ideas is a central protection afforded by the Constitution:

> It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective . . . restraint on freedom of association . . .. This Court has recognized the vital relationship between freedom to associate and privacy in one's associations * * *. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.[64]

Thus in Virginia, identifying persons supporting various causes treads upon Constitutional protections.

The Supreme Court of Virginia noted that among the factors controlling in federal decisions is whether there is "substantial relevancy" between the reasons for the disclosure requirement and the intrusion upon privacy of association reflected in anonymous participation.[65]

Narrowest Intrusion Upon Freedom of Expression. The Virginia Court also endorsed the "least restrictive means" requirement for any demand for disclosure of otherwise anonymous or private associations.[66] Thus the instrument of State action, whether judicial process or legislative enactment, must be specifically directed to acts or conduct which overstep legal limits, and not include those which keep within the protected area of free speech.[67] Further, the Court stressed the requirement of some preliminary showing of a "substantial connection" between the private identification information sought and the legitimate need to redress a wrong.[68]

---

[61] A.E. Dick Howard, Commentaries on the Constitution of Virginia, Volume I, Section 12, at p. 98.
[62] NAACP v. Committee on Offenses Against the Administration of Justice, 204 Va. 693, 698, 133 S.E.2d 540, 544 (1963).
[63] 204 Va. at 702, 133 S.E.2d at 546 (construing federal Constitutional principles).
[64] 204 Va. at 698-699, citing NAACP v. Alabama, 357 U.S. at 460.
[65] 204 Va. at 700, citing NAACP v. Alabama, 357 U.S. at 466.
[66] Id. at 701, quoting from Shelton v. Tucker, 364 U.S. at 488.
[67] Edwards v. Commonwealth, 191 Va. 272, 60 S.E.2d 916 (1950).
[68] Id. at 701, relying on Gibson, 372 U.S. at 558.

Other Principles. As the Supreme Court of Virginia has developed the law of freedom of speech and association, several generalizations have become apparent. One is that laws that affect fundamental constitutional rights are subjected to strict judicial scrutiny; the Court has held that discussion of public issues and debate on the qualifications of candidates for public office are integral to the operation of our system of government and are entitled to the broadest protection the First Amendment can afford.[69] Another basic principle is that expressions of opinion are protected by both the First Amendment to the Federal Constitution and Article I, Section 12 of the Constitution of Virginia,[70] and, therefore, generally cannot form the basis of a defamation action.[71]

Constitutional guarantees of free speech, have never been construed, however, to protect either criminal or tortious conduct.[72] As the Supreme Court has said, quoting federal authority:

> There are certain well-defined and narrowly limited classes of speech, the prevention and punishment of which has never been thought to raise any Constitutional problem. These include the lewd and obscene, the profane, the libelous, and the insulting or 'fighting' words -- those which by their very utterance inflict injury or tend to incite an immediate breach of the peace. It has been well observed that such utterances are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality.[73]

State enforced intrusions upon freedom of expression must have a reasonable basis in prevention of disorder, restraint of coercion, protection of life or property, or promotion of the general welfare.[74] And, measures regulating speech must be content neutral.[75] Finally, where a statute does not directly abridge free speech, but -- while regulating a subject within the State's power -- tends to have the incidental effect of inhibiting First Amendment rights, it is well settled that the statute can be upheld if the effect on speech is minor in relation to the need for control of the conduct and the lack of alternative means for doing so.[76]

Since the Virginia Bill of Rights provides as least as great, if not greater, protection of free speech than does the First Amendment, for convenience we will use the terms "First Amendment," "freedom of expression," and "free speech" to relate to ***both*** the federal and analogous Virginia constitutional protections of free speech, press, and association.

Right to Privacy – Limited Recognition in Virginia. One topic on which Virginia law provides less robust protections than federal law or that of other states is the right to

---

[69] Mahan v. NCPAC, 227 Va. 330, 315 S.E.2d 829 (1984).
[70] Williams v. Garraghty, 249 Va. 224, 455 S.E.2d 209 (1995).
[71] Chaves v. Johnson, 230 Va. 112, 119, 335 S.E.2d 97, 101-02 (1985).
[72] Id.
[73] McWhorter v. Commonwealth, 191 Va. 857, 63 S.E.2d 20 (1951).
[74] Edwards v. Commonwealth, 191 Va. 272, 60 S.E.2d 916 (1950).
[75] Adams Outdoor Advertising v. Newport News, 236 Va. 370, 373 S.E.2d 917 (1988).
[76] Freeman v. Commonwealth, 223 Va. 301, 288 S.E.2d 461 (1982).

privacy per se. Since 1980 virtually all American jurisdictions have come to recognize a right to relief expressly based upon invasion of a "right of privacy."[77] To date, a general right has not been recognized in the common law of Virginia. As summarized by the Supreme Court, "Virginia is among a few states, including New York, that recognizes a right of privacy [only] in a limited form by statute."[78] The protections available in Virginia for privacy concerns are embodied in Virginia in Code § 8.01-40(A), and in Virginia's Privacy Protection Act of 1976, former Code §§ 2.1-377 to –386 (*see* Code § 2.2-3800 et seq.). These enactments, along with relevant law on medical records privacy, do not have controlling significance for the present study, and are therefore discussed in Appendix A to this Report.

[77] Town & Country Properties, Inc. v. Riggins, 249 Va. 387, 394, 457 S.E.2d 356, 362 (1995), citing W. Page Keeton et al., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 849-51 (5th ed. 1984).
[78] 249 Va. at 394, 457 S.E.2d at 362.

V

IN CONTESTED APPLICATIONS TO PIERCE THE ANONYMITY OF PROTECTED COMMUNICATIONS IN CIVIL LITIGATION, A BALANCING TEST APPLIES: *ANALYSIS OF LIMITED CASE LAW, AND ANALOGIES TO SIMILAR SITUATIONS.*

A. Absence of Fully Articulated Statutory and Case Law on Identification Subpoenas

While Congress and the General Assembly have addressed the issue of liability of Internet service providers for the content of messages transmitted by their customers in the Communications Decency Act of 1996[79] and Virginia Code § 8.01-49.1[80] (effectively immunizing the provider from liability),[81] no federal legislation – and no Virginia statutory law – has addressed the standards for determining whether the identity of an otherwise anonymous communicator of electronic messages must be disclosed. As a result, attention must turn to Constitutional decisions and other case law that define the scope of protections for anonymous speech, and the adaptation of general doctrines in that context to the specific situation of anonymous Internet communications.

Piercing the Veil of Anonymity. The Supreme Court has emphasized that an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.[82] Anonymous pamphlets, leaflets, brochures and books have played an important role in the history and progress of mankind.[83] Disclosure requirements might provide assistance to critics in evaluating the quality and significance of a writing, but is not indispensable.[84] Drawing an analogy, the Court noted that "the now-pervasive practice of grading law school examination papers 'blindly' (i.e., under a system in which the professor does not know whose paper she is grading) indicates that such evaluations are possible -- indeed, perhaps more reliable -- when any bias associated with the author's identity is prescinded."[85] There is a respected tradition of anonymity in the advocacy of political causes, exemplified by the secret ballot, the right to vote one's conscience without fear of retaliation.

Flat Bans. Two state statutes that were interpreted as flatly banning certain forms of participation in anonymous communications on the Internet have been held unconstitutional in the only lower court decisions to address such provisions.[86] No appellate discussion of the anonymity provisions in particular has been forthcoming.[87]

---

[79] 47 U.S.C. § 230 et seq. See generally Appendix A to this Report.
[80] See Appendix A of this Report.
[81] Id. at § 230.
[82] McIntyre, 514 U.S. 334.
[83] See discussion in Part III above in this Report.
[84] McIntyre, 514 U.S. at 342.
[85] Id.
[86] See ACLU v. Miller, 977 F. Supp. 1228, 1232 (N.D. Ga. 1997) (stating that a Georgia "statute's prohibition of Internet transmissions which 'falsely identify' the sender constituted a presumptively invalid content-based restriction"); ACLU v. Johnson, 4 F.Supp.2d 1029, 1033 (D. N.M. 1998) (striking down a statute that prohibited

Specific Applications of Speech and Association Protections to Anonymous Electronic Messages. In connection with anonymous communications over the Internet, the U.S. Supreme Court has yet to apply or tailor the protections recognized and the level of scrutiny set forth in *Talley*, *Buckley* and *McIntyre* to civil litigation between two private actors. In general, of course, the Court's broad charter of Constitutional protection for the Internet in *ACLU v. Reno* makes it clear that traditional protections are fully available: a court must apply "exacting scrutiny," and will uphold the intrusion upon protected interests only if it is narrowly tailored to serve an overriding interest requiring disclosure.[88]

No state or federal appellate court has yet endorsed a particular formulation of the level of scrutiny or balancing test to be applied in this precise context, where the fundamental right of anonymous free speech is implicated in a ***private litigation*** where the identity of the author is arguably necessary to the outcome. In the one case to reach the Virginia Supreme Court arising from this subject matter, while the trial judge dealt extensively with the constitutional issues,[89] the appellate decision was devoted to consideration of the very distinct issues arising by legal claims launched by anonymous ***plaintiffs*** in inter-state litigations, rather than the applicable standards for compelled revelation of an anonymous ***communicator's*** identity.[90] Nonetheless the discussion in that case suggests some appropriate safeguards to be considered for the present topic as well, and these matters are set forth below.

In discussing granting enforcement to foreign discovery decrees under the doctrine of "comity" the Court indicated that such discovery demands from another jurisdiction are not to be "given effect when to do so would prejudice a State's own rights or the rights of its citizens."[91] While recognition of the validity of a foreign demand is a guiding principle, the Court noted that there are limitations on the application of comity: "Before according the privilege of comity, we have required a showing of [the foreign court's] personal and subject matter jurisdiction,[92] that "the procedural and substantive law applied by the foreign court [was] reasonably comparable to that of Virginia,"[93]that the decree was not "falsely or fraudulently obtained,"[94] that the order sought to be enforced was not "contrary to the morals or public policy of this State,"[95] and that the enforcement of the order would not "prejudice [Virginia's]

"people from communicating and accessing information anonymously"). See generally Lyrissa Lidsky, Silencing John Doe: Defamation & Discourse in Cyberspace, 49 Duke L.J. 855, n255 (2000).

[87] ACLU v. Johnson, 194 F.3d 1149 (1999), the appeal from the New Mexico federal trial court decision, affirmed the issuance of a preliminary injunction against enforcing the statute, but did not mention anonymity except in a passing reference summarizing the grounds for the trial court's decision.

[88] McIntyre, 514 U.S. 334.

[89] See In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26, 2000 Va. Cir. LEXIS 220 (Cir. Ct. Fairfax Cty. 2000).

[90] America Online, Inc. v. Anonymous Publicly Traded Co., 261 Va. 350, 542 S.E.2d 377 (described in Appendix B hereto).

[91] America Online, 261 Va. at 360-61, 542 S.E.2d at 283, citing McFarland v. McFarland, 179 Va. 418, 430, 19 S.E.2d 77, 83 (1942).

[92] Id., citing Oehl v. Oehl, 221 Va. 618, 623, 272 S.E.2d 441, 444 (1980).

[93] Id.

[94] Id., citing McFarland, 179 Va. at 430, 19 S.E.2d at 83.

[95] Id.

own rights or the rights of its citizens."[96] Whether the discovery demand was approved in an adversary proceeding, or only on an ex parte application in the foreign state was also noted as a factor.[97]

While the present study is not intended to provide a guide to the application of the First Amendment in the limitless range of conceivable circumstances for such disputes, some attention to the present understanding of the factors in the balance is necessary when formulating – as the General Assembly appears to contemplate – procedural legislation that bears on the information to be supplied in connection with subpoenas and related process litigated in Virginia courts. *In other words, the procedures must supply the appropriate courts with information necessary to decide whatever issues constitutional and tort law make relevant on the question of revealing the identities of anonymous communicators on the Internet.*

Thus, with due recognition of the risk that as the case law matures through the appellate process, different or additional considerations will be emphasized, it is prudent to study the efforts that have been made to date to grapple with this issue.

Efforts at the Trial Level to Define an Approach. Attempts to apply the prevailing constitutional standards in the specific context of disclosure of the identities of anonymous communicators over the Internet have been made by trial courts in Virginia,[98] and a handful of other jurisdictions. Two of the principal non-Virginia decisions, however, are skewed by a pre-litigation context that requires special focus on grounds for future federal court jurisdiction.[99] There is, therefore, a startling paucity of reported rulings on the precise issue considered in the present study.

The most prominent reported Virginia circuit court approach to this problem was applied by Judge Klein in *In re Subpoena Duces Tecum to America Online*,[100] where the court

---

[96] Id., citing Eastern Indem. Co. v. Hirschler, Fleischer, Weinberg, Cox & Allen, 235 Va. 9, 15, 366 S.E.2d 53, 56 (1988).

[97] 261 Va. at 361, 542 S.E.2d at 383.

[98] **Virginia**: See In re Subpoena Duces Tecum to America Online, 52 Va. Cir. 26, 36, 2000 Va. Cir. LEXIS 220, **21 (Cir. Ct. Fairfax Cty. 2000).

[99] **California and New Jersey.** A New Jersey state court adopted in Dendrite International v. Does, Dkt. No. MRS C-129-00 (N.J. Super. Ct. Ch. Div. Nov. 23, 2000), aff'd 2001 N.J. Super LEXIS 300 (2001) the four-part test suggested by a federal court in the Northern District of California. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999). This test requires the applicant for a subpoena to provide the court with (1) information about the unknown party to document that the person is a real individual or entity, (2) a listing of all prior steps to identify the unknown party, (3) a demonstration that plaintiff's underlying tort suit could withstand a motion to dismiss, (4) a copy of the discovery request, specifying the persons who are likely to have identifying information. Id. at 578-580. The New Jersey trial court found that the principals outlined in the Seescandy.com case were applicable and provided the parameters to be used in the balancing of interests. The court adopted and applied the four Seescancy.com parameters in their entirety. Dendrite, 2001 N.J. Super LEXIS at *23-25. **Washington State.** In Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (2001) (the court adopted the following standard for evaluating a civil subpoena that seeks the identity of an anonymous Internet user who is not a party to the underlying litigation, whether (1) the subpoena was sought in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) information sufficient to establish or to disprove that claim or defense is unavailable from any other source).

[100] 52 Va. Cir. 26, 2000 Va. Cir. LEXIS 220 (Cir. Ct. Fairfax Cty. 2000).

identified as controlling the issues of whether it has been shown that the applicant had a good faith basis for believing that he had been tortiously injured, and that identification of an Internet communicator was "centrally needed" to resolve his claim:

> [A] court should only order a non-party, internet service provider to provide information concerning the identity of a subscriber (1) when the court is satisfied by the pleadings or evidence supplied to that court (2) that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed and (3) the subpoenaed identity information is centrally needed to advance that claim.[101]

However, on appeal from the trial court proceedings in that case, the Supreme Court did not address either the procedural or the constitutional balancing issue.[102]

Other Virginia trial court cases involving anonymous communication have focused on other issues than those of interest in this Report.[103]

Other Jurisdictions. Nationally, only two "tests" have been reported. One is a California federal district court synthesis of the considerations that has also been applied by a New Jersey state trial court. This approach requires the applicant for a subpoena to provide the court with (1) information about the unknown party to document that the person is a real individual or entity, (2) a listing of all prior steps to identify the unknown party, (3) a demonstration that plaintiff's underlying tort suit could withstand a motion to dismiss, (4) a copy of the discovery request, specifying the persons who are likely to have identifying information.[104]

The other test was applied by a federal trial court in Washington state, which ruled that in evaluating a civil subpoena that seeks the identity of an anonymous Internet user who is not a party to the underlying litigation, the court should consider whether (1) the subpoena was sought in good faith and not for any improper purpose, (2) the information sought relates to a core claim or defense, (3) the identifying information is directly and materially relevant to that claim or defense, and (4) whether there is information sufficient to establish or to disprove that claim or defense is unavailable from any other source.[105]

While the federal trial decisions have not been the subject of an appellate opinion discussing or confirming the approach taken, the New Jersey trial court was affirmed in July of

---

[101] See In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26, 2000 Va. Cir. LEXIS 220 (Cir. Ct. Fairfax Cty. 2000).

[102] See Appendix B to this Report.

[103] See, e.g., In re Texaco, 51 Va. Cir. 411 (Loudoun Cty. 2000)(whether pre-litigation "perpetuation" of testimony for an expected lawsuit was appropriate); Melvin v. Doe, 49 Va. Cir. 257 (Loudoun Cty 1999)(question of minimum personal jurisdiction "contacts" with Virginia to allow personal jurisdiction).

[104] Northern District of California. Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999), applied in Dendrite International v. Does, Dkt. No. MRS C-129-00 (N.J. Super. Ct. Ch. Div. Nov. 23, 2000), aff'd 2001 N.J. Super LEXIS 300 (2001). See n. 100 above.

[105] In Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (2001).

2001 in an opinion which commended Judge Klein's approach in the Virginia case. The Appellate Division noted that a good approach stops short of a full "motion to dismiss" test for enforcement of a subpoena, and should be satisfied where there is sufficient showing of the bona fides of plaintiff's case to provide assurance that the discovery procedures to ascertain the identities of unknown defendants are not being undertaken to harass, intimidate or silence critics in the public forum opportunities provided by the Internet.[106]

Characterizing the balance to be struck. To generalize upon this limited body of case law, trial courts grappling with demands for identification of Internet communicators have generally concluded that the issue is to be resolved in civil cases[107] by placing the burden of going forward upon the party who seeks disclosure. When an initial showing of the prescribed form is made, an opportunity should be provided for the subpoenaed party and the anonymous person to file responses to the application, and when the record for decision is thus developed, the trial judge will be in a position to engage in the constitutional balancing required by the case law. The factors balanced in the small body of existing lower court case law have varied.[108]

Can the Issue be Avoided?

One Virginia trial judge has twice expressed the view that it may be desirable for the foreign jurisdiction where the case is pending to play a most central role in resolving identification disputes, and in one case expressed an inclination to physically send the disputed information, under seal, to the jurisdiction where the action is pending for decision. This approach recognizes that in the balancing of interests, once a subscriber is given notice the parties may wish to proceed (anonymously) in the court where the underlying lawsuit will be tried. This approach seeks to limit the possibility of multiple proceedings and appeals in two different jurisdictions, and the possibility that a case must be sent back to the underlying forum for factual findings needed to facilitate ruling on the subpoena in Virginia.

In one case the Loudoun County circuit court reviewed a subpoena application in which the plaintiff asserted that "without the information requested, the parties cannot be

---

[106] Dendrite International v. John Doe No. 3, 2001 N.J. Super. LEXIS 300 (July 11, 2001), discussing among other cases, Judge Klein's decision in In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26 (Va. Cir. Ct. 2000).

[107] See the Virginia criminal procedure provision concerning such disclosures, set forth in Part VI of this Report.

[108] In re Subpoena Duces Tecum to America Online, 52 Va. Cir. 26, 36, 2000 Va. Cir. LEXIS 220, **21 (Cir. Ct. Fairfax Cty. 2000) (requiring that the party requesting the subpoena has a "legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed, and the subpoenaed identity information is "centrally needed" to advance that claim); In re Subpoena Duces Tecum to America Online, Inc., 50 Va. Cir. 202, 203, 1999 Va. Cir. LEXIS 406, 4 (Cir. Ct. Loudoun Cty. 1999) (requiring that the information sought is "singularly relevant to the pursuit of the action and is reasonably calculated to lead to the discovery of admissible evidence."); Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999) and Dendrite International v. Does, Dkt. No. MRS C-129-00 (N.J. Super. Ct. Ch. Div. Nov. 23, 2000), aff'd 2001 N.J. Super LEXIS 300 (2001) (requiring that plaintiff's underlying tort suit be able to withstand a Motion to Dismiss); Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (2001) (requiring that the subpoena is sought is good faith and not for any improper purpose, the information sought relates to a core claim or defense, the identifying information is directly and materially relevant to that claim or defense, and information sufficient to establish or to disprove that claim or defense is unavailable from any other source).

identified."[109] The need for this basic information was obvious, and it met the test of "relevancy" applied in criminal cases in Virginia. The court also noted, however, that although the Louisiana court in which the underlying action was pending was not the exclusive forum for resolving privilege claims, in the instant case, it was the most appropriate. "Otherwise, this Court would be required to address matters going to the very heart of the claims in ancillary proceedings; that is, are these defendants shielded from claims of defamation by reason of a privilege arising out of the publication of documents over the Internet?"[110]

In another case, that same trial court indicated its "inclination" to order the information under subpoena to be produced to it under seal, and then forwarded to the Arkansas District Court, site of the underlying action, under seal, to await that court's ruling on a motion for protective order, effectively deferring the privacy determination to that court. The Virginia court invited comment by the Arkansas court on that mechanism.[111] In that litigation, however, the anonymous subscriber consented to proceeding in the foreign jurisdiction, and the federal court in the other jurisdiction approved of the procedure for forwarding documents under seal.

Judge Horne has aptly pointed out that many out-of-state subpoena requests are in aid of litigation elsewhere relating to local concerns in the other jurisdiction (e.g., an employee and an employer in another state are embroiled in a dispute relating to Internet communications). In those cases, once notice is provided to the subscriber of the subpoena request, counsel for the subscriber will be retained in the foreign jurisdiction where the underlying case is pending. In those instances, it may be more convenient for the parties to litigate all aspects of the dispute, including the anonymity issues, in that forum. Such a procedure, so long as it preserves the option of an Internet service provider which *elects* to file a motion to quash in Virginia to proceed here, may reduce the volume of contested applications embroiling service providers domiciled in Virginia and the courts of this Commonwealth.

Where such consent is not forthcoming, or where the service provider wishes to litigate in Virginia where it is headquartered, it is recommended in this Report that a policy of *renvoi* (sending back)[112] ***not*** be adopted as a general approach.

First, if the conditions necessary for recognition and enforcement of a foreign discovery request under the doctrine of comity are met, important policies concerning Virginia's role in the community of states suggest that sister-state process be honored.[113]

Second, a Virginia service provider could often be mightily burdened by the obligation to retain counsel, and transport knowledgeable personnel – and confidential business records – to another state, all to respond to a subpoena where the service provider is – by definition – not a party to the underlying dispute. It may well be that in the cases that have been considered to date in the Virginia trial courts, the service provider has been willing and able to litigate the

---

[109] In re Subpoena Duces Tecum to America Online, Inc., 50 Va. Cir. 202, 203, 1999 Va. Cir. LEXIS 406, 4 (Cir. Ct. Loudoun Cty. 1999).
[110] 50 Va. Cir. at 203.
[111] Life Plus International v. Doe, Misc. Law No. 23155 (Cir. Ct. Loudoun Cty. 2000)
[112] Sale v. Haitian Centers Council, 509 U.S. 155, 181-82 n. 37 (1993).
[113] See America Online, Inc. v. Anonymous Publicly Traded Co., 261 Va. 350, 542 S.E.2d 377 (2001).

disputes in as many states as necessary, but it would be poor policy to adopt a general rule encouraging trial courts entertaining subpoena disputes to require a Virginia company served with such a subpoena to do so. Perhaps a provision allowing such a move upon the uncoerced consent of all parties would address the issue.

Third, there is an argument that in some cases holding open the Virginia courts to hear the proceeding is required by the United States Constitution. Article IV, § 2 of the United States Constitution provides that the "Citizens of each State shall be entitled to all the Privileges and Immunities of Citizens of the several States." This clause, often called the "Interstate Privileges and Immunities Clause,"[114] was intended to "fuse into one nation a collection of independent states [by] insur[ing] to a citizen of State A who ventures into State B the same privileges which the citizens of State B enjoy."[115] Thus there may be a *right* of a citizen of another state to obtain a subpoena ruling and enforcement in Virginia if the Commonwealth provides that privilege to her own citizens. One restriction on the Constitutional argument, however, is that the clause is apparently applicable only to individuals: corporations are not "citizens" within the meaning of Article IV, § 2.[116]

One of the earliest interpretations of this doctrine concluded that among the fundamental protections the clause provides is the right "to institute and maintain actions of any kind in the courts of the state. . . "[117] The Privileges and Immunities Clause has thus been seen as a source of protection for citizens of *other states* against discrimination based on alienage, by providing that "whatever . . . rights [each state] grants . . . to [its] own citizens . . . shall be the measure of the rights of citizens of other states within [the forum state's] jurisdiction."[118]

While the Privileges and Immunities Clause does not prohibit Virginia from discriminating against citizens of other states in farming oysters,[119] it does protect basic rights of citizenship,[120] which appear to include access to the courts.[121] The leading case states that the right to sue and defend in the courts of the States is one of the privileges and immunities comprehended by § 2 of Art. IV, and that equality of treatment in regard thereto does not depend upon comity between the States, but is granted and protected by that provision in the Constitution; subject, however, to the restriction of that instrument that the limitations imposed by a State must operate in the same way on its own citizens and on those of other states.[122]

Thus, the Supreme Court has commented on occasion that "[t]he existence of . . . jurisdiction creates an implication of duty to exercise it,"[123] and that "a State may not evade the

---

[114] See Laurence H. Tribe, 1 American Constitutional Law § 6-36 at 1250 (3rd Ed. 2000)("Tribe").
[115] Toomer v. Witsell, 334 U.S. 385, 395 (1948).
[116] Tribe, § 6-36 at 1270 n. 99, citing Paul v. Virginia, 75 U.S. 168 (1869).
[117] Corfield v. Coryell, 6 Fed.Cas. 546, 551-53 (opinion of Justice Bushrod Washington, riding circuit, in 1823).
[118] Tribe, § 6-36 at 1253, quoting Conner v. Elliot, 59 U.S. 591, 593 (1856).
[119] McCready v. Virginia, 94 U.S. 391 (1876).
[120] Tribe, § 6-36 at 1254, 1259-61(the clause protects *at least* fundamental rights, and probably more).
[121] Corfield, 6 Fed.Cas. at 552-53.
[122] Chambers v. Baltimore and Ohio Railroad Company, 207 U.S. 142 (1907).
[123] Mondou v. New York, N. H. & H. R. Co., 223 U.S. 1, 58 (1912). See Testa v. Katt, 330 U.S. 386 (1947); Missouri ex rel. St. Louis, B. & M. R. Co. v. Taylor, 266 U.S. 200, 208 (1924); Robb v. Connolly, 111 U.S. 624, 637 (1884).

strictures of the Privileges and Immunities Clause by denying jurisdiction to a court otherwise competent."[124] The Supreme Court has stated generally that " the Privileges and Immunities Clause, Art. IV, § 2, secures to citizens of other states such right of access to the courts of a state as that state gives to its own citizens."[125] Indeed, there is also a Due Process argument that sometimes applies when a plaintiff is denied effective access to a forum.[126]

Of course, the Commonwealth's own policy may determine the jurisdiction of its courts and the character of the controversies that shall be heard therein,[127] though it seems obvious that Virginia would not require a Virginia resident serving a subpoena on a Virginia Internet service provider to travel to another state to litigate the enforceability of the subpoena.

Under the U.S. Supreme Court's current approach to Privileges and Immunities questions, proffered state justifications for differential treatment for the citizens of other states are considered. A "valid excuse" for not hearing the case will be recognized.[128] And "[w]hen a state court refuses jurisdiction because of a neutral state rule regarding the administration of the courts, [the Supreme Court] must act with utmost caution before deciding that it is obligated to entertain the claim.[129] "The States thus have great latitude to establish the structure and jurisdiction of their own courts,"[130] and differences and distinctions, even when applied to persons clearly protected by the Fourteenth Amendment, are not in themselves unconstitutional: "It is only when the variations are arbitrary and without reasonable legal basis that an unconstitutional discrimination occurs."[131]

Under existing precedent, a state may allow dismissal of an action by a foreign plaintiff against a foreign defendant, even though it would not countenance such a dismissal if the plaintiff were a citizen of the forum.[132] One could argue, *a fortiori*, that if an entire litigation between two non-citizens can be stricken from the Virginia court's docket, remitting a discovery dispute in a foreign action to the forum where the underlying litigation is pending cannot be impermissible.

Thus it is far from clear that it would be *unconstitutional* to erect a system of *renvoi* under which cases are routinely remitted to the jurisdiction where litigation on the merits is pending. However, for the reasons noted above, a general approach encouraging that process is

---

[124] Howlett v. Rose, 496 U.S. 356 (1990), citing Angel v. Bullington, 330 U.S. 183, 188-189 (1947); Douglas v. New York, N. H. & H. R. Co., 279 U.S. 377 (1929).
[125] Miles v. Illinois C. R. Co., 315 U.S. 698 (1942), citing Chambers v. Baltimore & Ohio R. Co., 207 U.S. 142, 148 (1907); McKnett v. St. Louis & S. F. Ry. Co., 292 U.S. 230 (1934).
[126] Compare Brinkerhoff-Faris Co. v. Hill, 281 U.S. 673 (1930) with Missouri v. Lewis, 101 U.S. 22, 30 (1879).
[127] Id.
[128] Howlett v. Rose, 496 U.S. 356, 369 (1990). See Douglas v. New York, N. H. & H. R. Co., 279 U.S. 377, 387-388 (1929) (Holmes, J.).
[129] Johnson v. Fankell, 520 U.S. 911, 919 (1997), citing Missouri ex rel. Southern R. Co. v. Mayfield, 340 U.S. 1 (1950); Georgia Rail Road & Banking Co. v. Musgrove, 335 U.S. 900 (1949) (per curiam); Herb v. Pitcairn, 324 U.S. 117 (1945); Douglas v. New York, N. H. & H. R. Co., 279 U.S. 377 (1929).
[130] Id.
[131] United States v. Burnison, 339 U.S. 87 (1950).
[132] Douglas v. New York, N.W. & H. R.R., 279 U.S. 377 (1929)(FELA action by Connecticut resident against a Connecticut corporation could be disallowed in New York state courts under state statute).

not attractive. Thus this Report will examine the analogies and other sources that suggest structures for deciding such disputes in the Virginia courts.

The proposed statute discussed later in this report, however, is not designed to preclude consensual procedures that bring the matter for disposition in the court where the underlying litigation is pending. Locating the decisionmaking in that court may help avoid situations in which the Virginia trial court could face evidentiary issues without meaningful mechanisms for testing credibility or other issues. One concern, noted by Judge Horne in considering a draft of this report, is that while a review of the face of pleadings may in some instances be sufficient to determine the viability of claims pending elsewhere, there can be cases in which factual issues of defense will play a controlling part, and in those instances involvement of the forum where the case will be tried could be most helpful.

B. **Analogous Disputes.**

Other, analogous situations exist in which lower courts have fashioned tests concerning disclosure of the identities of providers of information where constitutional doctrines generally provide some form of constitutional protection for maintaining anonymity. One analogy is the disclosure of the authorship of anonymous leaflet or advertising material. Another frequently discussed analogy concerns efforts to compel the news media to disclose the identity of journalistic sources.[133]

Revealing Authorship of Leaflets or Advertisements. In evaluating the constitutionality of statutes prohibiting anonymous leaflets or advertisements, the Supreme Court has evaluated both the ends that the statute is purported to achieve and the means by which the statute purports to achieve those ends, seeking to determine whether the governmental interest is sufficient to override the privacy interests at stake, and the intrusion narrowly limited to whatever is necessary to achieve the recognized needs for disclosure.[134] The Court, however, has not translated the general "strict scrutiny"/"compelling interest" approach of these cases to the context of identity disclosure demands arising in civil litigation. Thus these cases have not developed tests or discussions of principles directly applicable to the civil context now under consideration.

Revealing Journalistic Sources. While there are significant distinctions between the present context and disputes over disclosure of journalistic sources,[135] most observers have

---

[133] Another analogy might be an attorney's efforts to keep his client's identity confidential, most commonly in certain tax disputes. However, generally the identity of a client is not deemed confidential information, and "the opposing party has a right to know with whom he is contending or who the real party in interest is." R. M. Weddle, Annotation, Disclosure of Name, Identity, Address, Occupation, or Business of Client as Violation of Attorney-Client Privilege, 16 ALR 3d 1047 (1967).

[134] See discussion of *Talley* and *McIntyre*, supra at Part III of this Report.

[135] There are several reasons why this situation is a poor analogy. First, the tradition in American journalism has been to assure sources, when required, that their identities would not be revealed and that the reporters will gladly face jail on contempt rather then reveal a protected source. In contrast, the terms of service specified by many of the largest providers of Internet communication services expressly notify subscribers that information will be turned over in response to a subpoena. Second, there are "journalist-privilege" or "shield" statutes in a number of states, which create strong protections against revealing the sources of news stories. No such statutes directly address the identity of those posting electronic messages. Third, the context of journalist-source disputes is almost

considered such applications to present useful analogies. In particular, there is a body of lower court case law about the balancing required when a civil litigant demands identification of the anonymous speaker on whom the news media has relied.

While there is no shield statute in Virginia, the Supreme Court of Virginia has held that as a newsgathering mechanism, a newsman's privilege of confidentiality of information and identity of his source is an important catalyst to the free flow of information guaranteed by the freedom of press clause of the First Amendment.[136] Unknown at common law, it is a privilege *related to* the First Amendment and not a First Amendment right, absolute, universal, and paramount to all other rights.[137] In addressing the balancing of interests, the Court noted:

> [T]he privilege of confidentiality should yield only when the defendant's need is essential to a fair trial. Whether the need is essential to due process must be determined from the facts and circumstances in each case. We are of opinion that when there are reasonable grounds to believe that information in the possession of a newsman is material to proof of any element of a criminal offense, or to proof of the defense asserted by the defendant, or to a reduction in the classification or gradation of the offense charged, or to a mitigation of the penalty attached, the defendant's need to acquire such information is essential to a fair trial; when such information is not otherwise available, the defendant has a due process right to compel disclosure of such information and the identity of the source; and any privilege of confidentiality claimed by the newsman must, upon pain of contempt, yield to that right.[138]

The United States Supreme Court has never decided a case where the protection of an anonymous journalistic source was pitted against a request by a private plaintiff pursuing a defamation (or other tort) claim who asserted a need for identification of the speaker. In *Branzburg v. Hayes*[139], the Court did issue opinions in three collected cases which are taken as holding that there is no absolute "reporters' privilege" to withhold the identity of sources when demanded in a criminal law enforcement context by a grand jury.[140]

---

invariably that the source has provided information that at least some media actors have considered newsworthy, in the sense of addressing topics of public concern. No such assurance exists in the area of anonymous Internet e-mail and discussion postings. Hence it is not as uniformly clear in the present subject as it may be with journalist-privilege discussions, that the speech involved is in the highest or purest category of protected speech.

[136] Brown v. Commonwealth of Virginia, 214 Va. 755, 757, 204 S.E.2d 429, 431 (1974).

[137] Id.

[138] Id.

[139] 408 U.S. 665 (1972).

[140] See Id. The Supreme Court refused to find a privilege for a reporter to withhold from a grand jury the identity of his or her confidential sources. But Justice White, writing for a plurality of the Court, seemed to be balancing the need to protect sources with the need for grand juries to obtain information in these cases. The opinion concluded that the scales weighed in favor of disclosure because of the societal interest in ferreting out criminal behavior. Id at 690-91. Justice Powell, in a concurring opinion, explicitly called for a balancing of competing interests on a case-by-case basis. Id at 710. Echoing Justice Stewart's approach in Torre, Justice Powell said that a journalist could not be required to disclose information with respect to a confidential source if it is part of an effort at harassment or if it bore "only a remote or tenuous relationship to the subject of the investigation" or "without a legitimate need of law enforcement." Id. In a dissenting opinion in Branzburg, Justice Stewart argued for a qualified privilege against disclosure. He placed the burden on the government to overcome the privilege by showing that there is probable cause to believe that the reporter has information relevant to a "specific probable

The leading case on this issue in the civil tort context is the Second Circuit's decision in Garland v. Torre[141], where the court also found no constitutional privilege, and applied a balancing test to determine whether a journalist's confidential source must be disclosed. In an opinion written by Judge (later Justice) Stewart sitting by designation, the court recognized that "compulsory disclosure of a journalist's confidential sources of information may entail an abridgment" of a journalist's rights under the First Amendment.[142] In Garland, the court found that the balance was tipped in favor of the right of plaintiff to discover the source by the facts that other attempts to obtain the information had proven unavailing and that "[t]he question asked of [Torre] went to the heart of the plaintiff's claim."[143]

Since the protection for speech interests is "not an absolute", the court in Garland began with the premise that the constitutional protections existed to shield the identity of the news source, and then held: "What must be determined is whether the interest to be served by compelling the [disclosure] in the present case justifies some impairment of this First Amendment freedom."[144]

The Second Circuit in Garland expressly noted that the speech rights of a witness must give way to the duty to provide evidence to make the judicial process work fairly.[145] This follows, the court held, from the need of any civilized society to have an effective system for suing and defending in courts of law.[146] It would seem, *a fortiori*, that a ***defendant*** charged with tortious speech would have at least the speech burdens of a non-party witness, and hence that the balance in the cases which are the subject of this report would favor disclosure even more clearly.

Subsequent to Branzburg, and in light of the prominent decision in Garland, most courts that have faced the issue in a civil context have concluded that there *is* a First Amendment-based or common-law *qualified privilege* for a journalist to protect the identity of a confidential source during the course of libel litigation.[147]

---

violation of law," that the information sought could not be obtained by alternatives less destructive of the First Amendment rights, and that the government had a "compelling and overriding" interest in disclosure. Id. at 743.

[141] 259 F.2d 545 (2d Cir. 1958).

[142] Id. at 548.

[143] Id.

[144] Id.

[145] Id. at 549.

[146] Id. at 549: If an additional First Amendment liberty -- the freedom of the press -- is here involved, we do not hesitate to conclude that it too must give place under the Constitution to a paramount public interest in the fair administration of justice. 'The right to sue and defend in the courts is the alternative of force. In an organized society it is the right conservative of all other rights, and lies at the foundation of orderly government.' Chambers v. Baltimore & Ohio R. Co., 1907, 207 U.S. 142, 148. This, as Mr. Justice Frankfurter has pointed but in a somewhat different context, 'has nothing to do with curtailing expression of opinion, be it political, economic, or religious, that may be offensive to orthodox views. It has to do with the power of the state to discharge an indispensable function of civilized society, that of adjudicating controversies between its citizens and between citizens and the state through legal tribunals in accordance with their historic procedures.' Bridges v. State of California, 1941, 314 U.S. 252, 291 (dissenting opinion). See Patterson v. Colorado ex rel. Attorney General, 205 U.S. 454, 462-463 (1907).

[147] Robert D. Sack, SACK ON DEFAMATION, LIBEL, SLANDER AND RELATED PROBLEMS § 14.3.2, p. 14-10, 14-14 (3d ed. 2000) ("Sack, Defamation, Libel, Slander and Related Problems"). See, e.g., Zerilli v. Smith, 656 F.2d 705, 711-12 (D.C. Cir. 1981), citing Carey v. Hume, 492 F.2d 631, 636 (D.C. Cir.

As summarized by a leading treatise on defamation law, in cases where the identity of news sources is sought in a libel or slander action the plaintiff must make what is generally seen as a threefold showing before the journalist will be ordered to name his or her source:

- that the material to be disclosed is relevant [to a pending litigation?]
- that disclosure is essential to the plaintiff's claim, *i.e.*, that it goes "to the heart" of the plaintiff's case; and
- that there has been reasonable exploration, or exhaustion, of alternatives to such disclosure.[148]

Sometimes a fourth requirement is added: That the underlying claim, having been reviewed, has been found to have substance.[149] A plaintiff should be required to satisfy the court that the claims at issue are not frivolous before infringing on constitutionally based interests.[150]

In some cases, the record as developed through discovery makes it clear that the plaintiff will not be able to prevail at trial, regardless of whether he or she learns the identity of the reporter's confidential sources. In such cases, compelling disclosure is unnecessary and summary judgment for the defendant is appropriate.[151]

Of course, one prominent feature of the landscape in the journalists' privilege area is the presence of "shield" statutes in many jurisdictions, which prescribe procedures for the analysis of demands for disclosure of sources. For example, one Midwestern court read the state's shield statute and the federal constitutional case law together, and arrived at a five-step analysis.[152] The somewhat overlapping factors identified by the court were: (1) the nature of the litigation-that the party seeking protection is defending a public official or public figure defamation suit weighs in favor of disclosure; (2) relevance-does the information go to "the

---

1974)(determining whether the privilege applies requires courts to look to the facts of each case, weighing the public interest in protecting the reporter's sources against the private interest in compelling disclosure), citing Riley v. City of Chester, 612 F.2d 708, 715-16 (3d Cir. 1979) (upholding assertion of privilege); Silkwood v. Kerr-McGee Corp., 563 F.2d 433, 436-38 (10th Cir. 1978) (same); Baker v. F & F Investment, supra, 470 F.2d at 783 (same); Cervantes v. Time, Inc., 464 F.2d 986 (8th Cir. 1972) (same); Miller v. Transamerican Press, Inc., 621 F.2d 721, 725 (5th Cir. 1980) (ruling that privilege does not prevail). See also Democratic Nat'l Committee v. McCord, 356 F. Supp. 1394, 1398 (D.D.C.1973) (upholding privilege); Gulliver's Periodicals, Ltd. v. Chas. Levy Circulating Co., 455 F. Supp. 1197, 1203 (N.D.Ill.1978) (same); Altemose Construction Co. v. Building & Construction Trades Council of Philadelphia, 443 F. Supp. 489, 491 (E.D.Pa.1977) (same); Gilbert v. Allied Chemical Corp., 411 F. Supp. 505, 508 (E.D.Va.1976) (same).

[148] Sack, Defamation, Libel, Slander and Related Problems at p. 14-14.

[149] Id. at p. 14-15.

[150] See Miller v. Transamerican Press, Inc., 621 F.2d 721, mod., 628 F.2d 932 (5th Cir. 1980) ("Plaintiff must show substantial evidence that the challenged statement was published and is both factually untrue and defamatory..."); Mitchell v. Superior Court, 690 P.2d 625 (1984) (court may require plaintiff to make prima facie showing of falsity). See Sack, Defamation, Libel, Slander and Related Problems at p. 14-15. See also Romualdo P. Eclavea, Privilege of Newsgatherer against Disclosure of Confidential Sources of Information, 99 A.L.R.3d 37 (1980).

[151] Sack, Defamation, Libel, Slander and Related Problems at p. 14-16.

[152] Bauer v. Gannett Co., 557 N.W.2d 608 (Minn. Ct. App. 1997).

heart of the claim"; (3) availability of the information sought from alternative sources; (4) necessity of disclosure-may summary judgment for the defendant be warranted, for example, irrespective of the identity of the sources;[153] (5) the necessity of a prima facie showing of falsity of the allegedly defamatory statement by the plaintiff.[154] Some jurisdictions, by statute, limit the exceptions to their journalist "shield" statutes to information crucial to serious criminal cases, [155] or where a party can show that identification will demonstrate "actual malice" in a defamation case.[156]

The *Branzburg* ruling left open the possibility for state courts to construe "their own constitutions so as to recognize a newsman's privilege, either qualified or absolute.[157] Many states have enacted shield statutes to protect journalists from forced disclosure, reflecting a paramount public interest in the maintenance of a vigorous, aggressive and independent press capable of participating in robust, unfettered debate over controversial matters, an interest which has always been a principal concern of the First Amendment.[158] Although a few states have shield laws that provide journalists an absolute privilege, most states have a qualified privilege, which sets forth the circumstances and conditions under which news gatherers will be allowed to keep sources and information confidential. Examples of the absolute privilege can be found in Alabama and Pennsylvania. Both state statutes essentially protect journalists from being compelled to disclose their sources of information in any proceeding. The qualified privilege, on the other hand, varies from state to state, but most of the statutes require a First Amendment balancing test to determine whether the privilege applies to a given situation.[159]

---

[153] We should note that this approach is consistent with an often-cited canon of judicial approach, to the effect that rulings on constitutional issues should be avoided if the dispute can be appropriately resolved on non-constitutional grounds. Gomez v. U.S. 858, 864 (1989); Commodity Futures Trading Comm'n v. Schor, 478 U.S. 833, 841 (1986); United States v. Rumely, 345 U.S. 41, 45 (1953); Crowell v. Benson, 285 U.S. 22, 62 (1932).

[154] Sack § 14.3.4 at p. 14-22.

[155] The Minnesota statutes, at 595.024, for example provide that disclosure of an anonymous press informant "shall be granted only if the court determines after hearing the parties that the person making application, by clear and convincing evidence, has met all three of the following conditions:
(1) that there is probable cause to believe that the specific information sought (i) is clearly relevant to a gross misdemeanor or felony, or (ii) is clearly relevant to a misdemeanor so long as the information would not tend to identify the source of the information or the means through which it was obtained,
(2) that the information cannot be obtained by alternative means or remedies less destructive of first amendment rights, and
(3) that there is a compelling and overriding interest requiring the disclosure of the information where the disclosure is necessary to prevent injustice.

[156] Minn. Stat. § 595.025:
Subdivision 1. Disclosure prohibition; applicability. The prohibition of disclosure provided in section 595.023 shall not apply in any defamation action where the person seeking disclosure can demonstrate that the identity of the source will lead to relevant evidence on the issue of actual malice.
Subd. 2. Disclosure conditions. Notwithstanding the provisions of subdivision 1, the identity of the source of information shall not be ordered disclosed unless the following conditions are met:
(a) that there is probable cause to believe that the source has information clearly relevant to the issue of defamation;
(b) that the information cannot be obtained by any alternative means or remedy less destructive of first amendment rights.

[157] Laurence B. Alexander and Ellen M. Bush, Shield Laws on Trial: State Court Interpretation of the Journalist's Statutory Privilege, 23 J. Legis. 215, 217 (1997).

[158] Id.

[159] Id. at 218.

Subpoenas seeking testimony for identification of a confidential source get the strongest protection in states with shield laws.[160] Courts are more likely to recognize the privilege in states with absolute laws. Meanwhile, states with qualified shield laws may look to whether information is available elsewhere, balancing the public's need to know against the statutory and First Amendment rights of the reporter. For example, Tennessee and Illinois are examples of states that use a three-part test similar to the one suggested by Justice Stewart's dissent in *Branzburg v. Hayes*. These tests require courts to consider the importance of and the need for the information sought.[161]

Courts in states with absolute laws are more likely to quash subpoenas in libel cases than are courts in states with qualified laws.[162] Courts in Pennsylvania[163] and New Jersey[164] have upheld the media's right to keep source identification secret, even though the news organization was a defendant in a libel action. Although a New Jersey libel plaintiff claimed he could not go forward in his suit without discovery of sources, the New Jersey Supreme Court found the constitutional protection for freedom of speech outweighed the plaintiff's right to bring a libel action.[165] Despite the burden on some libel plaintiffs, the court said the First Amendment right to gather news and publish was more important than the right to bring a libel action.[166]

C. California's Anti-SLAPP approach.

The California legislature has taken a different approach in dealing with analogous issues, specifically with litigation that has come to be known as SLAPP, an acronym for "strategic lawsuits against public participation." Such suits are aimed at preventing citizens from exercising their political rights or punishing those who have done so.[167] A SLAPP suit has been defined as a meritless action, filed primarily to chill a defendant's exercise of First Amendment rights.[168] In enacting an "anti-SLAPP" statute, California Code of Civil Procedure § 425.16, that State's legislature concluded: "[T]here has been a disturbing increase in lawsuits

---

[160] Id. at 219.
[161] Id. at 220.
[162] Id.
[163] Sprague v. Walter, 543 A.2d 1078 (Pa. 1988); Hatchard v. Westinghouse Broadcasting Co., 504 A.2d 211 (Pa. 1986).
[164] Maressa v. New Jersey Monthly, 445 A.2d 376 (N.J. 1982).
[165] Id. at 387.
[166] Id. See also, House of Wheat v. Wright, slip opinion (Ohio Ct. App. 1985) (the court held that the shield privilege is absolute in civil litigation and upheld the denial of discovery of sources where a funeral home director sued a television station for libel); Jamerson v. Anderson Newspapers, 469 N.E.2d 1243, 1248 (Ind. Ct. App. 1984) (a libel plaintiff argued that the court should presume that a defendant who refuses to reveal sources has no sources so that both sides are even in the discovery process. The court held that such a presumption would "emasculate the protection afforded by the shield law," noting the law says that no inference may be drawn from the invocation of privilege). But see, Alexander & Bush, 23 J. Legis. at 221 (Some qualified shield laws specifically exempt use of the law in a libel case. Minnesota, Oklahoma, Oregon, Rhode Island and Tennessee simply do not allow the press to use the shield law in a libel or slander action where it is the defendant); Id. at 226 (Because of the difference in shield law language and in how state courts interpret them, the effectiveness of shield laws varies tremendously from state to state).
[167] Wilcox v. Superior Court of Los Angeles County, 27 Cal. App. 4th 809, 815 (1994).
[168] Id.

brought primarily to chill the valid exercise of the constitutional rights of freedom of speech and petition for the redress of grievances. The Legislature finds and declares that it is in the public interest to encourage continued participation in matters of public significance, and that this participation should not be chilled through abuse of the judicial process."[169]

This California Code provision authorizes a "special motion to strike" an alleged SLAPP suit on the pleadings and declarations of the parties. It applies to causes of action "against a person arising from any act of that person in furtherance of the person's right of petition or free speech under the United States or California Constitution in connection with a public issue."[170] The procedure employed under this California enactment amounts to an early summary judgment hearing (it is conducted upon the pleadings, affidavits and memoranda of the parties) in which the plaintiff must demonstrate that there is "a probability that the plaintiff will prevail on the claim."[171] The focus of the statute is lawsuits arising from statements "made in a place open to the public or a public forum in connection with an issue of public interest."[172] The motion to strike must be filed within 60 days of the service of the complaint unless permission of court is obtained to file it later, and all discovery proceedings in the action are stayed upon the filing of such a motion.

Despite the statutory language requiring a plaintiff to establish a probability that he will prevail on the claim to survive the special motion to strike, the statute provides that this burden does not arise unless the claim is one falling within the ambit of the statute, i.e. that the suit was "brought primarily to chill the valid exercise of the constitutional rights of freedom of speech and petition for the redress of grievances" "in connection with a public issue."[173] Thus as the California system actually operates, the defendant in an alleged SLAPP suit bears the initial burden of showing that the suit falls within the class of suits subject to the special motion to strike.[174]

Another concern about the California approach is that it does not provide adequate assistance to courts reviewing subpoenas for identities of anonymous Internet posters. While discovery is stayed during pendency of the special motion to strike, and thus a court would not be required to act on the subpoena request, the anti-SLAPP statute does not provide for a mechanism for notice to an anonymous defendant that the lawsuit is pending. Without notice, an anonymous defendant will be unable to file a special motion to strike, and stay the court's decision on the subpoena request. Courts are given no guidance as to how to handle subpoena requests in this setting, when the defendant has not been afforded the opportunity to file a special motion to strike.

Given the focus of the study resolution, which recognizes that the large majority of the most difficult "motions arise out of cases pending in other states but are being heard in the Commonwealth solely because the Internet service providers (ISPs), which may be the

---

[169] Cal. Code Civ. Proc., § 425.16(a).
[170] Cal. Code Civ. Proc., § 425.16(b)(1).
[171] Id.
[172] Cal. Code Civ. Proc., § 425.16(e)(3).
[173] Cal. Code Civ. Proc., § 425.16(a), (b).
[174] Wilcox, 27 Cal. App. 4th at 819.

custodians of such electronic data, are located in the Commonwealth,"[175] the merits of the underlying litigation are not presented to the Virginia courts in these cases. Hence an anti-SLAPP statute is not proposed in the present Report.

[175] The full text of the Study Resolution is set forth in Part I of this Report.

VI

HOW THE SUBPOENA PROCESS CURRENTLY OPERATES IN VIRGINIA

A. Federal Discovery and Subpoena Practice

Federal courts in Virginia (and across the Nation) can obtain disclosure of information from Virginia Internet service providers via the federal discovery Rules (FRCP 26-37) if the service provider is a "party" to the federal litigation, and under Rule 45 if the provider is a non-party to the underlying lawsuit.

Discovery from Parties. Parties in federal litigation are obligated to respond to the same five discovery devices recognized in Virginia (depositions, document production, interrogatories, requests for admissions and physical/mental examinations). Where a corporate entity is a party to federal litigation, as in Virginia practice the federal courts will enforce discovery requests for information in the custody or control of the party. If a category of information – to pick a relevant example, confidential client identification data – is objected to, the federal rules contemplate protection for privileged information[176] and a specification by the responding party that it is withholding particular responsive data on grounds of such a claim of confidentiality.[177] Typically, a "log" of withheld items is prepared to facilitate any motion practice contesting the propriety of the claim of confidentiality.[178]

Subpoenas to Non-Parties. Under Rule 45, the federal courts may issue subpoenas to non-parties for any producible information. Since 1991, this Rule has permitted attorneys for a party to issue subpoenas on behalf of the court where the action is pending, and such process is enforceable in any federal court in the United States. Thus, for example, a subpoena issued in connection with litigation pending in San Francisco can be enforced in a Virginia federal court against a non-party located in Virginia. While the Virginia subpoenaed party cannot normally be compelled to travel to the distant forum, or bear unreasonable expense, production of information here in Virginia where the subpoenaed party has its offices is normal.[179]

Effect of State Law. Federal courts employ federal procedure, even in cases where state law supplies the rule of decision on the merits.[180] State privilege law, however, is normally recognized, and a Virginia individual or entity can raise both federal and state privilege doctrines, among other defenses, to the enforcement of a federal subpoena.[181]

---

[176] See F.R.C.P. 26(b)(scope of discovery in federal courts includes "any matter, not privileged") and 26(c) (protective orders).

[177] F.R.C.P. 26(b)(5).

[178] See, e.g., In re Pfohl Bros. Landfill Litig., 175 F.R.D. 13 (W.D. N.Y. 1997) (Rule 26(b)(5) requires that the party asserting the privilege or protection must specifically identify each document or communication, and the type of privilege or protection being asserted, in a privilege log).

[179] See generally Kent Sinclair, FEDERAL CIVIL PRACTICE (3d ed.) at p. 717-19.

[180] See Erie R.R. Co. v. Tompkins, 304 U.S. 64 (1938); Sibbach v. Wilson & Co., 312 U.S. 1 (1941); Semtek Int'l Inc. v. Lockheed Martin Corp., 531 U.S. 497 (2001).

[181] See Kent Sinclair, FEDERAL CIVIL PRACTICE (3d ed. 1998) at p.740-41.

As a result of these doctrines, there is some significance in the characterization of any Virginia state statute or rule governing disclosure of the identity of anonymous Internet communicators: if the matter is deemed purely "procedural," it will govern cases in the courts of the Commonwealth, but not proceedings in the federal courts. However, if the governing provision is seen as a substantive protection of rights, akin to a traditional privilege or "shield statute," it should be recognized as governing proceedings in federal court.[182]

B. Virginia State Subpoena Practice: Information from Non-Parties

Discovery from parties under Part Four of the Rules of Court is not the topic of the present Study Resolution, and has been sketched in various publications.[183]

Subpoena Mechanism. The provision of current Virginia discovery rules pertaining to subpoenas for information held by non-parties is Rule 4:9(c). The controlling principles have not changed under this Rule for decades, but it was amended effective July 1, 2000 by addition of provisions for "attorney-issued subpoenas" (not requiring action by a judge or clerk of court).

The pertinent provisions of Rule 4:9(c) call for "dispatch"[184] of a properly issued subpoena to a non-party, designating and describing the information sought, and specifying a place and time for compliance with the demand; an opportunity for objection and/or modification of the subpoena is provided. The key portion of the Rule reads:

> **(c) Production by a Person Not a Party. -**
>
> **(1) Subpoena duces tecum issued by clerk of court.** - Upon written request therefore filed with the clerk of the court in which the action or suit is pending by counsel of record for any party or by a party having no counsel in any pending case, with a certificate that a copy thereof has been mailed, dispatched by commercial delivery service, or transmitted by facsimile, or delivered to counsel of record and to parties having no counsel, the clerk shall, subject to paragraph (c-1), issue to a person not a party therein a subpoena duces tecum which shall command the person to whom it is directed, or someone acting on his behalf, to produce the documents and tangible things (including writings, drawings, graphs, charts, photographs, phono-records, and other data compilations from which information can be obtained, translated, if necessary, by the respondent through detection devices into reasonably usable form) designated and described in said request, and to permit the party filing such request, or someone acting in his behalf, to inspect and copy, test, or sample any

---

[182] See, e.g., Ramey v. Kingsport Publishing Corp., 905 F.Supp. 355 (W.D. Va. 1995)(applying the Virginia privilege of "fair report" in a defamation context, and citing Fourth Circuit precedent for doing so).

[183] See generally Kent Sinclair and Leigh Middleditch, VIRGINIA CIVIL PROCEDURE (3rd Ed. 1998) § 12.

[184] Under amendments to the Virginia Rules of Court effective February 1, 1999, the subpoena may be served on the person from whom information is sought by "delivering, dispatching by commercial delivery service, transmitting by facsimile or mailing a copy to each counsel of record on or before the day of filing.

> tangible things which constitute or contain matters within the scope of Rule 4:1(b) which are in the possession, custody or control of such person to whom the subpoena is directed, at a time and place and for the period specified in the subpoena; but, the court, upon written motion promptly made by the person so required to produce, or by the party against whom such production is sought, may (1) quash or modify the subpoena if it is unreasonable and oppressive, (2) condition denial of the motion to quash or modify upon the advancement by the party in whose behalf the subpoena is issued of the reasonable cost of producing the documents and tangible things so designated and described or (3) direct that the documents and tangible things subpoenaed be returned only to the office of the clerk of the court through which such documents and tangible things are subpoenaed in which event, upon request of any party in interest, or his attorney, the clerk of such court shall permit the withdrawal of such documents and tangible things by such party or his attorney for such reasonable period of time as will permit his inspection, photographing, or copying thereof.

Under the July 1, 2000 amendments to this rule, an attorney may "issue" the subpoena without involving the clerk in that process.[185]

The Virginia rules of Court are silent about the procedure for implementing the right set forth in the Rule as quoted above to file a motion to quash or modify a subpoena. In a leading case, the Supreme Court emphasized that it is the subpoenaed person's responsibility to lodge such an application, and that simply failing to respond is not appropriate.[186] Contempt is an available remedy where there is a failure to comply with a properly issued and served subpoena,[187] and even where a subpoena is served one workday before information must be provided, the option of unilateral non-compliance is not available.[188]

---

[185] Rule 4:9(c)(2) provides:
In a pending civil proceeding, a subpoena duces tecum may be issued by an attorney-at-law as an officer of the court if he is an active member of the Virginia State Bar at the time of issuance. An attorney may not issue a subpoena duces tecum in those civil proceedings excluded in Virginia Code 8.01-407. An attorney-issued subpoena duces tecum must be signed as if a pleading and be accompanied on the subpoena by the attorney's address, telephone number and Virginia State Bar identification number. A copy of any attorney-issued subpoena duces tecum must be mailed or delivered to the clerk's office of the court in which the case is pending by the attorney on the day of issuance with a certificate that a copy thereof has been mailed, dispatched by commercial delivery service, transmitted by facsimile, or delivered to counsel of record and to parties having no counsel. If time for compliance with an attorney-issued subpoena duces tecum is less than fourteen (14) days after service of the subpoena, the person to whom the subpoena is directed may serve on the party issuing the subpoena a written objection setting forth any grounds upon which such production, inspection or testing should not be had. If an objection is made, the party issuing the subpoena shall not be entitled to the requested production, inspection or testing, except pursuant to an order of the court in which the civil proceeding is pending. If an objection is made, the party issuing the subpoena may, upon notice to the person to whom the subpoena is directed, move for an order to compel the production, inspection or testing. Upon a timely motion, the court may quash, modify or sustain the subpoena as provided above in subsection (c)(1) of this Rule.
[186] Bellis v. Commonwealth of Virginia, 241 Va. 257, 402 S.E.2d 211 (1991).
[187] Id. at 262.
[188] Id. at 261.

Comparison to Other Systems for Notice and Objection. Certain other procedural rules, state and federal, deal in part with the option for a person to object and seek the quashing of an information demand by an elaborate notice of rights, and invitation to make prompt written objection, even by a lay person.

For example, Federal Rule 45 requires that each subpoena carry printed on its face a warning to the person who is named that there are rights to object. The federal language provides that subpoena must contain the following text:

> Subject to paragraph (d)(2) of this rule, a person commanded to produce and permit inspection and copying may, within 14 days after service of the subpoena or before the time specified for compliance if such time is less than 14 days after service, serve upon the party or attorney designated in the subpoena written objection to inspection or copying of any or all of the designated materials or of the premises. If objection is made, the party serving the subpoena shall not be entitled to inspect and copy the materials or inspect the premises except pursuant to an order of the court by which the subpoena was issued. If objection has been made, the party serving the subpoena may, upon notice to the person commanded to produce, move at any time for an order to compel the production. Such an order to compel production shall protect any person who is not a party or an officer of a party from significant expense resulting from the inspection and copying commanded.[189]

In Virginia, when certain forms of medical record disclosure are sought, the patient must be provided with a form of notice that educates him or her about the right to object and the procedure. Virginia Code § 32.1-127.1:03 (H) requires that the following language be included in a notice to the patient when his records have been subpoenaed:

> If you believe your records should not be disclosed and object to their disclosure, you have the right to file a motion with the clerk of the court to quash the subpoena...
>
> If you elect to file a motion to quash, you must notify your doctor or other health care provider(s) that you are filing the motion so that the provider knows to send the records to the clerk of court in a sealed envelope or package for safekeeping while your motion is decided.

Application to Subpoenas in Virginia Seeking Identification of Internet Communicators. Because the procedural rules and statutes in the Commonwealth do not themselves specify the nature of required submissions, the judges fielding these subpoenas and the associated objection proceedings have created and applied, ad hoc, the procedures and required submissions standards discussed previously in this Report.[190]

Criminal Case Analogy. Virginia has enacted a statute to deal with the discovery of electronic data in the criminal context.[191] While no Supreme Court or Court of Appeals

---

[189] F.R.C.P. 45 (c)(2)(B).

[190] See Part V of this Report.

[191] Code § 19.2-70.3 provides:

decision has been reported interpreting this statute, the standard articulated, "relevant to a legitimate law enforcement inquiry" may provide inadequate guidance to trial courts reviewing subpoena requests A balancing test, as proposed herein in the civil context, may also be the preferred approach in criminal cases. In application, the public interest in criminal law enforcement may weigh more heavily in favor of disclosure in criminal cases. However, it does not follow that a balancing of interests is any less necessary or appropriate in the criminal context than it is in the civil context.

A. A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service, excluding the contents of electronic communications, to an investigative or law-enforcement officer only pursuant to:

1. A subpoena issued by a grand jury of a court of this Commonwealth;
2. A search warrant issued by a magistrate, general district court or a circuit court;
3. A court order for such disclosure issued as provided in this section; or
4. The consent of the subscriber or customer to such disclosure.

B. A court shall issue an order for disclosure under this section only if the investigative or law-enforcement officer shows that there is reason to believe the records or other information sought are relevant to a legitimate law-enforcement inquiry. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify the order, if the information or records requested are unusually voluminous in nature or compliance with such order would otherwise cause an undue burden on such provider.

C. No cause of action shall lie in any court against a provider of a wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant or subpoena under this section.

VII

PROPOSED SYNTHESIS AND DRAFT RULE/STATUTE

A. Overview of the Burdens of Production and Persuasion

Presumption of Protection; Overview of the Shifting Burdens. (1) The anonymity of a communicator on the Internet is presumed to be Constitutionally protected at the outset;[192] (2) a party demanding identification of the communicator must carry the burden of making an initial showing (producing the underlying pleadings or evidence)[193] which is calculated to show eligibility for judicial assistance in the form of a subpoena, and to provide the court with information necessary in assessing the application.[194] (3) If such an application is filed, a subpoena will issue.[195] (4) Pursuant to timelines to be prescribed, the subpoenaed party must be given an opportunity to transmit copies of the subpoena to the anonymous subscriber involved, and (5) both the subscriber and the service provider (and any other person with standing) must be afforded an opportunity to respond to the subpoena by objection or motion for a protective order or motion to quash, making factual, procedural, statutory or constitutional arguments for partial or complete relief from the obligation to provide the information demanded. (6) Compliance with the subpoena must be deferred until a final ruling on the pending dispute, which may in some circumstances include the opportunity for appellate review.[196] (7) The judge reviewing a contested subpoena will balance the need for the information sought, as shown in the applicant's submissions, and the interests weighing against disclosure as reflected in any opposition, and apply the constitutional test of *Talley*, *McIntyre* and the related cases.[197]

---

[192] This premise is consistent with the history of constitutional protection for anonymous speech, recounted in Part II of this Report. It also places the burden of producing some evidence on the shoulders of the party who would pierce that protection.

[193] Judge Klein has used phraseology calling for satisfactory "pleadings or evidence supplied to [the] court." In re Subpoena Duces Tecum to America Online, 52 Va. Cir. 26, 37, 2000 Va. Cir. LEXIS 220, **24 (Cir. Ct. Fairfax Cty. 2000).

[194] Comments received from America Online relating to the study resolution noted that some applications may be lodged with incomplete information. Of particular concern were attorney-issued subpoenas. Study of attorney-issued subpoenas, however, led the General Assembly to experiment with this process for two years and then, in 2000-2001, to adopt the process on an ongoing basis. In practice, attorney-issued subpoenas under Rule 4:9(c)(2) and Code § 8.01-407 have not generated any significant abuse in Virginia to date. AOL is no doubt correct in envisioning occasional subpoena applications that do not contain all categories of information listed in the draft statute in this report. The present proposed legislation, however, does not call for any change in the general procedures by which subpoenas are issued in Virginia (except, perhaps, in insisting that a copy of all subpoenas in the subject area addressed herein be filed promptly with the court). Thus, attorney-issued subpoenas will be prepared by counsel and tested by the court if objection is lodged. Subpoenas issued by the clerk of court are fairly routinely promulgated in Virginia, though a clerk of court or circuit court judge may on occasion review and deny or modify an application. The present report does not specify any heightened level of pre-service review of the subpoenas in this subject area.

[195] Va. Sup. Ct. R 4:9(c)(2) and Code § 8.01-407.

[196] America Online, Inc. v. Anonymous Publicly Traded Company, 261 Va. 350, 542 S.E.2d 377 (2001) (for appellate review in an inter-state case, before according comity, personal and subject matter jurisdiction must be shown, as well as reasonable comparability of the procedural and substantive law applied by the foreign court, that the decree was not falsely or fraudulently obtained, the order sought was not contrary to the state's morals or public policy, and its enforcement would not prejudice the state or the rights of its citizens).

[197] See Part III of this Report for a summary of these doctrines.

In keeping with the focus of the Study Resolution, the discussion in this section of the report – and the draft statute set forth below – are intended to address only those situations in which private litigants in civil cases seek information relating to anonymous online communicators by serving a subpoena on the communicator's Internet service provider. The proposal does not relate to criminal cases, administrative subpoenas, or entities other than those providing Internet services[198] (for example, an employer who maintains information about employee e-mail accounts). The legislation would address requests for information about current or past customers of Internet service providers, to the extent that the provider happens to retain any information about the account.

B. The Applicant's Showings.

Extent of the Applicant's Proof Burdens. (a). The showings that an applicant must make can be defined by category, but the level of proof required is *as* important or *more* important than the topics themselves. Thus, much of the existing body of case law recognizes a threshold concern that the applicant indicate **(a) that one or more communications that are [or may be] tortious or illegal have been made by the anonymous person**. Whether this must be "suggested," "shown," "demonstrated," etc., and at what level assurance, will have a dramatic effect on the number and efficacy of the applications. Probably the best approach to this issue is the language used in some existing Virginia trial court case law on point, calling for a showing "that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed." This formulation avoids the impractical and inappropriate spectacle of the local judge responding to a contested subpoena request attempting to rule on the ultimate merits of a nascent lawsuit, perhaps a litigation in a foreign forum applying the substantive tort law of another jurisdiction.

Other formulations of the strength of this showing use the concept of the claim being capable of withstanding a motion to dismiss (or demurrer).[199] That standard is less desirable, for it requires a definitive ruling from the court entertaining the subpoena application on the viability vel non of the underlying lawsuit. The good faith basis test suggested above allows reasoned adjudication without turning the Virginia proceeding into a final decision on the merits of the action, in a factual vacuum and applying what may be unfamiliar legal principles.

(b). Other suggested elements of the required showing help complete the context needed to rule on the pending subpoena, and provide assurance that makes it more reasonable to rely on only a prima facie or preliminary demonstration of the validity of the claim on the merits. Thus, existing trial court responses to these issues suggest that the applicant should show **that other efforts using reasonable diligence to identify the anonymous communicator have proven fruitless**. This modest exhaustion requirement is consistent with the notion that there should be a real need for information before the protection for anonymous speech is assailed.

---

[198] For example, the legislation presumably should include entities such as "Yahoo!", which provides mail services for customers, though there may be no direct "service" provided in the sense of basic internet access.

[199] See Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999); Dendrite International v. Does, Dkt. No. MRS C-129-00 (N.J. Super. Ct. Ch. Div. Nov. 23, 2000), aff'd 2001 N.J. Super LEXIS 300 (2001).

(c). A key showing called for in the trial court decisions rendered to date is some indication of **the importance of the identity to the resolution of the underlying claims.** Some decisions talk in terms of a required showing that the information sought is centrally needed to advance that claim.[200] That test appears to be derived from cases involving the disclosure of confidential sources in news source defamation litigation.[201] Another test would be whether "the information sought relates to a core claim or defense."[202] A third variation, calls for a showing that "the identifying information is directly and materially relevant to that claim or defense."[203] Given the fact that proving "malice" or other scienters relevant in modern defamation law[204] is a central concern, identifying the individual and conducting further discovery into that person's knowledge and motivations may be so imperative in importance that fine-tuning of the phraseology of this issue will not affect the outcome in many cases. Similarly, considerations of enforcement of the court's judgment suggest that identification of the actor, if the allegations are not terminated adversely to the plaintiff, will become a necessity at some stage.

However, in designing a procedural statute or rule there is no need to adopt a specific *level* of importance that must be shown. Under prevailing constitutional rules, the court ruling upon the contested subpoena will be required to balance the need for the information against the constitutional values implicated in the anonymity of the communicator. Hence it will be in the adversarial interest of the application to make whatever showing is available about the significance of the identifying information, and whether that showing is "core", "central" or otherwise speaks to matters the judge is best equipped to deal with in performing the constitutional balance. Thus in framing a rule or statute dealing with such applications the most sensible approach may be to highlight the issue of "importance" more generally, and allow evolving advocacy, changes in case law, and the facts of each case to determine how much of a showing the applicant can make, to feed into the balance the judge must make concerning the right of anonymous speech.

(d). A fourth requirement, also consistent with the notion that constitutional conflicts should be avoided if possible, is **that the actionability of the communications cannot be**

---

[200] In re Subpoena Duces Tecum to America Online, 52 Va. Cir. 26, 36, 2000 Va. Cir. LEXIS 220, 21 (Cir. Ct. Fairfax Cty. 2000).

[201] See, e.g., Garland v. Torre, 259 F.2d 545, 548 (2d Cir. 1958), *cert denied*, 358 U.S. 910 (1958) (must "go to the heart of the plaintiff's claim"); Branzburg v. Hayes, 408 U.S. 665, 710 (1972) (disclosure not required if it bears "only a remote or tenuous relationship to the subject of the investigation" or "without a legitimate need of law enforcement"); Sack, Defamation, Libel, Slander and Related Problems § 14.3.2, p. 14-14 (3d ed. 2000) (generally, plaintiff must make a threefold showing before the journalist will be ordered to name his or her source: (1) that the material to be disclosed is relevant; (2) that disclosure is essential to the plaintiff's claim, i.e., that it goes 'to the heart' of the plaintiff's case; and that there has been reasonable exploration, or exhaustion, of alternatives to such disclosure. Sometimes a fourth requirement is added: That the underlying claim, having been reviewed, has been found to have substance. Id. at 14-15).

[202] Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (2001).

[203] In re Subpoena Duces Tecum to America Online, Inc., 50 Va. Cir. 202, 203, 1999 Va. Cir. LEXIS 406, 4 (Cir. Ct. Loudoun Cty. 1999) ("The talisman for judging the instant request is the badge of relevancy."); Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (2001) (the identifying information sought is directly and materially relevant to that claim or defense).

[204] See generally Sack, Defamation, Libel, Slander and Related Problems, ch. 2 (3d ed. 2000).

determined while the author remains anonymous, [i.e., that no motion to dismiss, motion for judgment on the pleadings or judgment as a matter of law, demurrer or summary judgment-type motion challenging the viability of the lawsuit of the underlying plaintiff is pending or imminent]. Concededly, a structure that places the onus on the discovery applicant to make this representation suffers from the anomaly that this party will typically be *the plaintiff* in the pending tort suit, and hence not the party who may be contemplating a dispositive motion to knock out the claims as not actionable as, say, defamation. However, even if this requirement becomes, in practice, little more than an assurance to the Virginia trial court that there is no summary judgment or motion to dismiss pending in the underlying case, it will help assure that efforts of the Virginia judge are not expended on the eve of a potential dismissal of the underlying claims by the court with jurisdiction over the merits of the case.

(e). Another practical requirement that appears appropriate is that **the applicant shall provide the court with a statement indicating why the persons to whom the subpoena is addressed are likely to have responsive information.**[205] Where the recipient is an Internet service provider it seems likely that the provider will have some identifying information, though the last address on file with the provider may, of course, have become out of date.

(f). To facilitate understanding and weighing of all the foregoing factors, and the constitutional balancing to come, **the applicant must lodge a copy of the discovery request (the proposed subpoena and any attachments thereto).**[206]

(g). The specification of submissions should be left open-ended such that in any given case the demanding party is free to supply additional pertinent information in support of the subpoena application.

Other Considerations. While the additional considerations mentioned by the Supreme Court of Virginia in its most recent "comity" decision do not need to be set forth in specific factors for consideration of the trial court in responding to a subpoena, it bears noting that these considerations could, in a given case, suggest grounds for denying enforcement of a foreign subpoena. Those factors include: whether the foreign court has personal and subject matter jurisdiction over the action out of which the discovery demand arises,[207] whether the procedural and substantive law applied by the foreign court is reasonably comparable to that of Virginia,[208] whether any order endorsing the discovery demand was approved in an adversary proceeding, or only on an ex parte application in the foreign state,[209] and whether enforcement order would prejudice Virginia's rights or the rights of its citizens."[210]

---

[205] Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 580 (1999) (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).

[206] See Va. Sup. Ct. R 4:9(c) for procedural requirements.

[207] Id., citing Oehl v. Oehl, 221 Va. 618, 623, 272 S.E.2d 441, 444 (1980).

[208] Id.

[209] 261 Va. at 361, 542 S.E.2d at 383.

[210] Id., citing Eastern Indem. Co. v. Hirschler, Fleischer, Weinberg, Cox & Allen, 235 Va. 9, 15, 366 S.E.2d 53, 56 (1988).

The handful of existing trial court decisions are naturally affected by the specific litigation postures of the cases that were pending before these courts when the identification issue arose. Various elements of the tests mentioned by these courts can be omitted in generalizing the issues. Other elements mentioned in some decisions are either covered, or obviated, by considerations already discussed under slightly different rubrics. For example, at least one court asked for a showing that "the subpoena was sought in good faith and not for any improper purpose".[211] Such a showing is subsumed in the demonstration that the information cannot be located elsewhere and addresses an important topic in resolving the litigation. A federal court dealing with pre-litigation discovery required "information about the unknown party to document that the person is a real individual or entity,"[212] a requirement that does not have general application in a system without the constraints of the diversity of citizenship requirements of the federal courts or the vicissitudes of discovery before action under Federal Rule 27. Hence no general need for applications addressing that factor has been ascertained.

C. Responsibilities and Options of the Subpoenaed Person

The person who is subpoenaed has both rights and responsibilities. As a Virginia person or entity, the subpoenaed person – in a fundamental sense – owes the people its evidence. Just as witnesses to a traffic accident have the obligation to give evidence upon request, a person or entity that has custody of confidential information must cooperate with the legal processes.

In the case of confidential identity information concerning an Internet communicator, there are several sources of obligation bearing upon the holder of the information. One source of duties is the contract (often called "terms of service" in this context) between the Internet service provider and the customer who would prefer to communicate anonymously on the electronic media.

Other obligations arise from the jurisdiction and power of the court system, attained by proper service of a properly issued piece of compulsory process – the subpoena. Even as a non-party, the subpoenaed person must respond (by production, objection or other application) even if the subpoena is overbroad, or burdensome.[213]

The subpoenaed person has correlative rights, as well. In some instances the subpoenaed person may take a neutral stance, but in others that person may object to the discovery demand embodied in the subpoena, on a wide range of grounds. Burdens to the subpoenaed party are fully cognizable in an application for relief (quashing or modifying a subpoena).

In addition, better practice will be for the Commonwealth to accord standing to the subpoenaed person, if so advised (based on its legal interests, contractual obligations with its

---

[211] See, e.g., In re Subpoena Duces Tecum to America Online, 52 Va. Cir. 26, 36, 2000 Va. Cir. LEXIS 220, 21 (Cir. Ct. Fairfax Cty. 2000); Doe v. 2TheMart.com Inc., 140 F. Supp. 2d 1088 (2001).
[212] Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999).
[213] Bellis, 241 Va. 257, 402 S.E.2d 211.

own customers, or other considerations) to object to the subpoena and seek its quashing or modification based upon the intrusion upon customer or subscriber rights entailed in compliance with the subpoena. Particularly with respect to Internet service providers, who are much more likely to be sophisticated entities and "repeat players" in the subpoena process, the capacity and interest to make a challenge on behalf of a particular customer or subscriber may be present. Since the interests of the subscribers, most of whom are lay individuals, are of constitutional stature, and the court system has an interest in full presentation of the relevant arguments, it is preferable to empower the service providers with the option to make objections and seek relief from subpoenas in light of their clients' interests as well as their own.

D. Submissions by the Subpoenaed Party or Anonymous Communicator

The procedure for adjudication of contested subpoenas must permit responses by subpoenaed parties, as well as the anonymous communicator.

Any subpoenaed party has the opportunity to object on a variety of grounds to a third-party subpoena. Examples under the Federal Rules of Civil Procedure include when the subpoena fails to allow a reasonable time for compliance, when it requires disclosure of privileged or other protected matter and no exception or waiver applies, and when it subjects a person to undue burden.[214] Courts may examine material about which a claim of privilege has been asserted to determine whether in fact the privilege exists.[215] In camera review, however, is not required and is not to be used as a substitute for a party's obligation to justify the withholding of documents.[216]

Determining what constitutes an undue burden is a matter of discretion on the part of the court.[217] Examples of undue burden might include untimely service, inability to produce the requested documents or things, failure to identify items requested, excessive cost, or a subpoena that is overbroad on its face.[218] The burden of proving that a subpoena is unduly burdensome in on the party requesting relief from the production obligation.[219] The party requesting relief cannot rely on a mere assertion that compliance would be burdensome without showing the manner and extent of the burden and the injurious consequences of insisting upon compliance.

Under Rule 45 of the Federal Rules of Civil Procedure, motions to quash, modify, or condition the subpoena are to be made to the court from which the subpoena issued, rather than to the court in which the underlying action is pending.[220] It is the issuing court that has the necessary jurisdiction over the party issuing the subpoena and the person served with it to

---

[214] Fed. R.Civ. P. 45(c)(3)(A).
[215] 9 James Wm Moore, et al., MOORE'S FEDERAL PRACTICE p. 45-38 (3d ed. 1997).
[216] Id.
[217] Id. at 45-39.
[218] Id. at 45-40.
[219] Id. at 45-41.
[220] 9A Charles A. Wright & Arthur R. Miller, FEDERAL PRACTICE AND PROCEDURE p. 40-41 (2d ed. 1969).

enforce the subpoena.[221] While not binding on state courts, this approach is a sensible one and one that favors enforcement of valid subpoenas.

Because of the sophistication of many Internet service providers, these entities should be permitted (though not required by law) to make objections on constitutional grounds on behalf of their subscribers.[222] The terms of service in the contract between the subscriber and the service provider will in many cases control what action, if any, the provider undertakes. From the standpoint of designing a procedural statute to protect the interests of Internet communicators, many of whom it is fair to assume are individuals without legal training or sophistication, it will be beneficial on balance to empower the provider – if it chooses to do so – to offer whatever arguments on the merits of the subpoena dispute it wishes.

Procedures for simplified objection by the subscriber should also be included; a notice, not unlike the concept of the notice that accompanies federal subpoenas under Rule 45, has been drafted to provide warning and an advice of rights for those who are the targets of such a subpoena. A simplified objection form for pro se response has also been drafted, as an illustration of the range of possible protections. In order to deter baseless objections, however, the objection procedure should require a written statement, in detail, of all grounds for relief upon which the anonymous communicator relies, and that the various factors discussed in case law as being helpful or necessary for the trial courts to consider in assessing the disclosure obligation be addressed in any objection lodged.

The description of information to be invited in opposition to a subpoena is not susceptible to the definitive categorization that should govern the applications for subpoenas. It does seem, however, that in defamation cases at least some invitation should be made for the objecting parties to identify the reasons that anonymity is desired, and whether the subject matter of the communications concerns topics of "public interest" as to which the Supreme Court has attached a presumption of greater protection for speech.[223] To the extent that the prima facie or facial plausibility of the plaintiff's claims must be reviewed by the court, the opponents of the subpoena should be free to provide information about the "public figure" status of the plaintiff, and any other characterizations made relevant by governing defamation or other tort law domains, such as whether the assailed communication is a matter of "fact" or "opinion" for purposes of the law of defamation.

---

[221] Id.

[222] See Part VI of this Report, where standing to object is discussed.

[223] See New York Times Co. v. Sullivan, 376 U.S. 254, 266, 270-71 (1964); Bigelow v. Virginia, 421 U.S. 809, 822 (1975); Rosenbloom v. Metromedia, 403 U.S. 29, 43 (1971).

Draft Legislation. A statutory implementation of these concerns could follow this illustrative format.

§ XXX Privilege for Anonymous Communication; Grounds for Piercing Privilege.

A. Information identifying any such anonymous participant in communications is presumed confidential, and shall not be disclosed by its custodians pursuant to a civil subpoena issued by a court of the Commonwealth except in accord with this section or with the consent of the anonymous communicator.

B. It is the intention of this section that the privilege for anonymous communications and grounds for exception to its application set forth in this section be applicable in all litigations, state or federal, involving information held by an individual or entity domiciled in Virginia. In cases where disclosure of identifying information is sought, the following procedure shall apply:

1. At least 30 days prior to the date on which disclosure is sought, a party seeking information identifying an anonymous communicator shall file with the appropriate circuit court a complete copy of the subpoena and all items annexed or incorporated therein, along with supporting material showing:

(a) that one or more communications that are or may be tortious or illegal have been made by the anonymous person, or that the party requesting the subpoena has a legitimate, good faith basis to contend that it is the victim of conduct actionable in the jurisdiction where suit was filed. A copy of the communications which are the subject of the action or subpoena shall be submitted.

(b) that other reasonable efforts to identify the anonymous communicator have proven fruitless.

(c) that the identity of the anonymous communicator is important, *i.e.*, is centrally needed to advance the claim, relates to a core claim or defense, or is directly and materially relevant to that claim or defense.

(d) that no motion to dismiss, motion for judgment on the pleadings, or judgment as a matter of law, demurrer or summary judgment-type motion challenging the viability of the lawsuit of the underlying plaintiff is pending. The pendency of such a motion may be considered by the court in determining whether to enforce, suspend or strike the proposed disclosure obligation under the subpoena.

(e) that the individuals or entities to whom the subpoena is addressed are likely to have responsive information.

(f) If the subpoena sought relates to an action pending in another jurisdiction, the application shall contain a copy of the pleadings in such action, along with the mandate, writ or commission of the court where the action is pending that authorizes the discovery of the information sought in Virginia.

2. Two copies of the subpoena and supporting materials set forth in subsection (B)(1)(a)-(e) shall be served upon the person to whom it is addressed along with payment sufficient to cover postage for remailing of one copy of the application within the United States, registered and with return receipt.

3. Within five business days after receipt of a subpoena application calling for disclosure of identifying information concerning a client, subscriber or customer, the individual

or entity to whom the subpoena is addressed shall (i) send an electronic mail notification to such person reporting that the subpoena has been received if an e-mail address is available, and (ii) dispatch one copy thereof, by registered mail or commercial delivery service, return receipt requested, to that client, subscriber or customer at his or her last known address (if any is on file with the person to whom the subpoena is addressed).

4. At least five business days prior to the date on which disclosure is sought under the subpoena, any interested person may file a detailed written objection, motion to quash, or motion for protective order. Any such papers filed by the anonymous client, subscriber or customer shall be served on or before the date of filing upon the party seeking the subpoena and the party to whom the subpoena is addressed. Any such papers filed by the party to whom the subpoena is addressed shall be served on or before the date of filing upon the party seeking the subpoena and the client, subscriber or customer whose identifying information is sought. Service is effective when it has been mailed, dispatched by commercial delivery service, or transmitted by facsimile, or delivered to counsel of record and to parties having no counsel.

5. Any written objection, motion to quash, or motion for protective order shall set forth all grounds relied upon for denying the disclosure sought in the subpoena, and shall also address to the extent feasible (i) whether the identity of the anonymous communicator has been disclosed in any way beyond its recordation in the account records of the party to whom the subpoena is addressed, (ii) whether the subpoena fails to allow a reasonable time for compliance, (iii) whether it requires disclosure of privileged or other protected matter and no exception or waiver applies, or (iv) whether it subjects a person to undue burden.

6. The party to whom the subpoena is addressed shall not comply with the subpoena earlier than three business days before the date on which disclosure is due, to allow the anonymous client, subscriber or customer the opportunity to object. If any person files a written objection, motion to quash, or motion for protective order, compliance with the subpoena shall be deferred until the appropriate court rules on the obligation to comply. If an objection or motion is made, the party serving the subpoena shall not be entitled to inspect and copy the materials except pursuant to an order of the court on behalf of which the subpoena was issued. If an objection or motion has been made, the party serving the subpoena may, upon notice to the person commanded to produce, move at any time for an order to compel the production. Two copies of any such motion to compel shall be served upon the subpoenaed party, who shall mail one copy thereof, by registered mail or national commercial delivery service, return receipt requested, to the client, subscriber or customer whose identifying information is the subject of the subpoena at that person's last known address.

C. The party requesting or issuing a subpoena for information identifying an anonymous Internet communicator shall serve along with each copy of such subpoena notices in boldface capital letters in substantially this form:

NOTICE TO INTERNET SERVICE PROVIDER

WITHIN 5 BUSINESS DAYS AFTER RECEIPT OF THIS SUBPOENA CALLING FOR IDENTIFYING INFORMATION CONCERNING YOUR CLIENT, SUBSCRIBER OR CUSTOMER, YOU ARE REQUIRED BY CODE § XXX TO MAIL ONE COPY THEREOF, BY REGISTERED MAIL OR NATIONAL COMMERCIAL DELIVERY SERVICE, RETURN RECEIPT

REQUESTED, TO THE CLIENT, SUBSCRIBER OR CUSTOMER WHOSE IDENTIFYING INFORMATION IS THE SUBJECT OF THE SUBPOENA. AT LEAST 5 BUSINESS DAYS PRIOR TO THE DATE ON WHICH DISCLOSURE IS SOUGHT YOU MAY, BUT ARE NOT REQUIRED TO, FILE A DETAILED WRITTEN OBJECTION, MOTION TO QUASH OR MOTION FOR PROTECTIVE ORDER. ANY SUCH OBJECTION OR MOTION SHALL BE SERVED UPON THE PARTY INITIATING THE SUBPOENA AND UPON THE CLIENT, SUBSCRIBER OR CUSTOMER WHOSE IDENTIFYING INFORMATION IS SOUGHT.

IF YOU CHOOSE NOT TO OBJECT TO THE SUBPOENA, YOU MUST ALLOW TIME FOR YOUR CLIENT, SUBSCRIBER OR CUSTOMER TO FILE HIS OR HER OWN OBJECTION, THEREFORE YOU MUST NOT RESPOND TO THE SUBPOENA ANY EARLIER THAN THREE BUSINESS DAYS BEFORE THE DISCLOSURE IS DUE.

IF YOU RECEIVE NOTICE THAT YOUR CLIENT, SUBSCRIBER OR CUSTOMER HAS FILED A WRITTEN OBJECTION, MOTION TO QUASH OR MOTION FOR PROTECTIVE ORDER REGARDING THIS SUBPOENA, OR IF YOU FILE A MOTION TO QUASH THIS SUBPOENA, NO DISCLOSURE PURSUANT TO THE SUBPOENA SHALL BE MADE EXCEPT PURSUANT TO AN ORDER OF THE COURT ON BEHALF OF WHICH THE SUBPOENA WAS ISSUED.

NOTICE TO INTERNET USER

THE ATTACHED PAPERS MEAN THAT _____ (INSERT NAME OF PARTY REQUESTING OR CAUSING ISSUANCE OF THE SUBPOENA) HAS EITHER ASKED THE COURT TO ISSUE A SUBPOENA, OR A SUBPOENA HAS BEEN ISSUED, TO YOUR INTERNET SERVICE PROVIDER _____(INSERT NAME OF INTERNET SERVICE PROVIDER) REQUIRING PRODUCTION OF INFORMATION REGARDING YOUR IDENTITY. UNLESS A DETAILED WRITTEN OBJECTION IS FILED WITH THE COURT, THE SERVICE PROVIDER WILL BE REQUIRED BY LAW TO RESPOND BY PROVIDING THE REQUIRED INFORMATION. IF YOU BELIEVE YOUR IDENTIFYING INFORMATION SHOULD NOT BE DISCLOSED AND OBJECT TO SUCH DISCLOSURE, YOU HAVE THE RIGHT TO FILE A DETAILED WRITTEN OBJECTION OR MOTION WITH THE CLERK OF THE COURT TO QUASH THE SUBPOENA OR TO OBTAIN A PROTECTIVE ORDER. YOU MAY ELECT TO CONTACT AN ATTORNEY TO REPRESENT YOUR INTERESTS. IF YOU ELECT TO FILE A WRITTEN OBJECTION, MOTION TO QUASH, OR MOTION FOR PROTECTIVE ORDER, IT SHOULD BE FILED AS SOON

AS POSSIBLE, AND MUST IN ALL INSTANCES BE FILED NO LESS THAN FIVE BUSINESS DAYS BEFORE THE DATE ON WHICH DISCLOSURE IS DUE (LISTED IN THE SUBPOENA). IF YOU ELECT TO FILE A WRITTEN OBJECTION OR MOTION AGAINST THIS SUBPOENA, YOU MUST AT THE SAME TIME SEND A COPY OF THAT OBJECTION OR MOTION TO BOTH YOUR INTERNET SERVICE PROVIDER AND THE PARTY WHO REQUESTED THE SUBPOENA.

IF YOU WISH TO OPPOSE TO THE ATTACHED SUBPOENA, IN WHOLE OR IN PART, YOU OR YOUR ATTORNEY MAY FILE WRITTEN OBJECTIONS OR A MOTION TO QUASH THE SUBPOENA, OR YOU MAY USE THE FORM BELOW, WHICH MUST BE FILED WITH THE COURT AND SERVED UPON THE PARTY REQUESTING THE SUBPOENA AND THE INTERNET SERVICE PROVIDER BY MAILING AT LEAST FIVE BUSINESS DAYS PRIOR TO THE DATE SET IN THE SUBPOENA FOR DISCLOSURE:

_____

Name of Court Listed on Subpoena

_____

Name of Party Seeking Information

Case No. _____

OBJECTION TO SUBPOENA DUCES TECUM

I object to the Subpoena Duces Tecum addressed to _____ for the following reasons:

[Name of Internet Service Provider to Whom the Subpoena is Addressed]

_____

(Please PRINT. Set forth, in detail, all reasons why the subpoena should not be complied with, and set forth, in addition, state (i) whether the identity of the anonymous communicator has been disclosed in any fashion, (ii) whether the subpoena fails to allow a reasonable time for compliance, (iii) whether it requires disclosure of privileged or other protected matter and no exception or waiver applies, or (iv) whether it subjects a person to undue burden.)

_____

_____

_____

_____

_____

_____

_____

(attached additional sheets if needed)

Respectfully Submitted,
John Doe _____
Enter e-mail nickname or other alias used in communicating via the Internet service provider to whom the subpoena is addressed.

CERTIFICATE

I hereby certify that a true copy of the above Objection to Subpoena Duces Tecum was mailed this _____ day of _____, (month, year), to

_____
(Name and address of party seeking information)

and

_____
(Name and address of Internet Service Provider)

John Doe _____
Enter e-mail nickname or other alias used in communicating via the Internet service provider to whom the subpoena is addressed.

[NOTE: in comments on a draft of this Report, America Online has suggested that the option for filing a "simple" objection may invite too many rote subscriber objections. AOL proposed, therefore, that the objection option be dropped. In its stead, AOL suggested the creation of a procedure similar to one used in some federal appellate courts, in which the subscriber would file a "simple" or "informal" brief, and that the applicant for the subpoena would respond with an "informal" brief. The trial court judge would then determine whether the dispute can be determined on the abbreviated papers before the court, or whether to direct the preparation and submission of more formal and elaborate briefing.

The AOL comments on this point appear to focus on the need to assure that only serious claims of confidentiality lead to motion practice (which is inherently burdensome for the service providers, and of course for the courts as well). The federal appellate "informal briefing" procedure is not necessarily unworkable. However, it is not similar to general practice in the Virginia trial courts and may have the result of fending off some ill-considered or knee-jerk objections at the expense of burdening the trial court with two waves of briefing on such applications (the informal first wave, and more complete briefing if the court so directs).

In this report, the concern expressed by AOL has been addressed by specifying that any objection must be in writing, must be "detailed," and must set forth all grounds for opposing the subpoena. In addition, the example form has been beefed up with a direction that the written objections must address several factors which the case law has made relevant to the court's decision of such disputes.

CONCLUSION

A. Is a Uniform Statewide Procedure Desirable?

The significance of Internet communications, and the freedom of expression rights of the federal and Virginia Constitutions that underlie such communications, suggest that fundamental societal values are at stake in the encouragement of unfettered expression through the medium of anonymous Internet speech.[224] Given the national trend toward increased litigation about anonymous communications, and the burdens these lawsuits impose on the trial courts, explicit guidance and clear procedures appear highly desirable. Particularly with respect to litigations pending in another jurisdiction, the task of a Virginia judge is complicated, with two procedural systems at work, and foreign substantive law normally controlling the merits. The fact that the anonymous communicators are often laypersons with little access to legal representation complicates the picture still further. Normal subpoena practice does not assure the interested parties any significant "lead time" for evaluation, objection and response. This factor alone argues for a procedure that allows contestants and custodians of the information sought to have a commercially reasonable timetable that avoids undue burdens while providing timely resolution of legal challenges. All of these considerations suggest that a specific procedure should be adopted for addressing subpoenas for information identifying anonymous Internet communicators.

Because constitutional interests are involved, and because the General Assembly has evidenced in the present Study Resolution and other enactments that it is concerned that Virginia remain among the Nation's most hospitable environments for the development and use of electronic media, it seems highly appropriate that legislation be considered to make certain

(A) that the Commonwealth's citizens have the full protections the Virginia and federal Constitutions provide to them, and an appropriate and fair opportunity to protect those rights; and

(B) that enterprises who possess identifying information be protected from unnecessary entanglement with litigations, and are compelled to make disclosure only when proper standards have been met; and

(C) that the Commonwealth's judges are provided with the information they need for full and fair consideration of the relevant factors in ruling on such disputes.

B. Self-Regulation by the Internet Services Market: the Contract Approach

Proponents of a market-oriented approach to regulation of Internet use and anonymity have suggested both that current legal rules simply do not apply to cyberspace, and that they

[224] See Part III of this Report.

are unnecessary.[225] Commentators favoring self-regulation encourage the establishment of "anonymity contracts" which would govern the level of acceptable anonymity on the Internet. Proponents of self-regulation argue that the market will set the amount of anonymity allowed in cyberspace in these contracts, at the amount desired by the cyberspace public, the optimal level.[226]

Under this approach, the Internet service provider could outline specific rules and policies and each subscriber would be required to agree to follow the rules or risk losing anonymity.[227] The service provider could choose whether to allow anonymous messages at all, and if they are allowed, could create as many restrictions as desired.[228] The market would be free to dictate the status of anonymity. The contracts that users enter would reflect the public perception of anonymity's usefulness.[229] If the Usenet community believes that anonymity should be highly regulated and restricted in certain newsgroups, then services that offer more relaxed standards would not exist.[230]

However, advocates of this approach fail to demonstrate the reliability of the market in addressing the specific problem of constructing the appropriate balance between the benefits of anonymity and the need for accountability in cyberspace.[231] The principal concern would be that those persons injured by illegalities perpetrated under the cloak of anonymity would not necessarily be parties to the suggested anonymity contracts.[232] Victims of defamation and other civil wrongs have no way of making their preferences heard or heeded in an anonymity contract market. For them, more is needed than a market-oriented approach to protection.

C. Statute vs. Rule.

Rules of Court govern the subpoena process in Virginia, and there are many reasons why Virginia's Supreme Court, which promulgates the Rules of Court, should remain responsible for shaping the procedures. The Court maintains an elaborate system of advisory committees with members from all corners of the Virginia litigation landscape: plaintiffs and defense practitioners, civil and criminal law experts, judges at all of the levels of the Virginia system, and clerks of court. The Judicial Council, which reviews the work of the committees, contains an equally diverse representation of judicial personnel, bar leaders and legislators. The multi-step process engaged in by the rules drafting bodies, including in recent years the commitment to publish in statewide legal papers all substantive proposals, has resulted in an open system that collects and analyzes information from practicing lawyers and sitting judges

---

[225] Noah Levine, Note: Establishing Legal Accountability for Anonymous Communication in Cyberspace, 96 Colum. L. Rev. 1526 (1996).
[226] Id. at 1538.
[227] George P. Long, III, Symposium: Comment: Who Are You?: Identity and Anonymity in Cyberspace, 55 U. Pitt. L. Rev. 1177.
[228] Id. at 1201.
[229] Id. at 1202.
[230] Id.
[231] Levine, 96 Colum. L. Rev. at 1539.
[232] Id.

across the Commonwealth, and shapes the procedural rules to attain the goals of uniformity with fairness.

The particular topic of this Study Resolution is narrow, focused as it is on the situation where a single form of confidential information is sought using the compulsion of the subpoena mechanism. As a result, it is recommended in this Report that the specific needs of that context be addressed in legislation tailored to the topic at hand. Such a proposal is set forth in the previous section of this Report. Whether any changes in the Rules of Court would be wise for the broader run of situations in which subpoenas are issued for information held by persons in Virginia, is a matter best left to the Rules committees. Since statutes prevail over any inconsistent provision of the Rules,[233] the legislative goals will be met in this approach.

D. Standing

In fashioning a procedure for challenges to subpoenas seeking confidential information maintained by Internet service providers, it appears to be the best policy to deem service providers to have standing – along with the anonymous Internet communicators who are the subscribers – to raise issues with respect to legal demands for production of information the providers maintain. This approach best serves the important speech interests which are implicated.

In one reported Virginia trial court decision, the issue of standing was litigated to the ruling stage.[234] An out-of-state litigant seeking to enforce a subpoena directed to a Virginia-based service provider argued that "if the subpoena unreasonably burdens the First Amendment rights of the John Does, then the John Does are the proper parties to seek relief from the subpoena, not [the service provider]." The trial court held that this argument "ignores longstanding precedent upholding the standing of third parties to seek vindication of First Amendment rights of others in situations analogous to the circumstances presented herein."[235]

The trial court opinion, which was not disturbed on appeal in this respect,[236] noted that in a landmark case[237] the United States Supreme Court rejected Alabama's argument that the NAACP lacked standing to assert the constitutional rights of its members, holding that the entity "argues more appropriately the rights of its members, and that its nexus with them is sufficient to permit that it act as their representative before this Court."[238] One factor identified by the U.S. Supreme Court was the fact that compelled disclosure would have a direct effect on the organization itself:

---

[233] See Code 8.01-4.
[234] In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26, 31-32, 2000 Va. Cir. LEXIS 220, **12-**15 (Cir. Ct. Fairfax Cty. 2000).
[235] Id.
[236] See America Online, Inc. v. Anonymous Publicly Traded Co., 261 Va. 350, 542 S.E.2d 377.
[237] NAACP v. Alabama, 357 U.S. 449 (1958).
[238] In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. at 31-32, 2000 Va. Cir. LEXIS 220 at **13-**14, citing NAACP, 357 U.S. at 458-59.

> The reasonable likelihood that the Association itself through diminished financial support and membership may be adversely affected if production is compelled is a further factor pointing towards our holding that petitioner has standing to complain of the production order on behalf of its members.[239]

Similarly, the Supreme Court of Virginia ruled in another landmark decision[240] that an organization had standing to take legal steps to maintain the confidentiality of its member and donor lists, reasoning that:

> There can be no reasonable doubt that a disclosure of the names of those who support the activities of the appellants could have no result other than to injuriously affect the effort of appellants to obtain financial support in promoting their aims and purposes.[241]

The recent Virginia circuit court opinion addressing these matters found that it "cannot be seriously questioned that those who utilize the "chat rooms" and "message boards" of [an Internet service provider] do so with an expectation that the anonymity of their postings and communications generally will be protected. If [the service provider] did not uphold the confidentiality of its subscribers, as it has contracted to do, absent extraordinary circumstances, one could reasonably predict that . . . subscribers would look to [the service provider's] competitors for anonymity. As such, the subpoena duces tecum at issue potentially could have an oppressive effect on [the service provider that contested it]."[242]

Another consideration in according standing to the commercial entity which maintains the data is "whether all, or any, of the subscribers [have the] financial ability to defend against the subpoenas."[243] The thoughtful circuit court judge concluded, as the Supreme Court has noted, that "when the right to anonymity is at issue, 'to require that [the right] be claimed by the members themselves would result in nullification of the right at the very moment of its assertion."[244] Hence, the circuit judge held that the Internet service provider had standing to assert the First Amendment rights of John Doe subscribers whose identifying information was sought.

The proposed Virginia electronic disclosure rule adopts a similar approach, according the right to pursue objections to a subpoena to ***both*** the anonymous subscriber and the service provider.

---

[239] NAACP, 357 U.S. at 459-60.

[240] NAACP Legal Defense and Educ. Fund, Inc. v. Committee on Offenses Against the Admin. of Justice, 204 Va. 693, 133 S.E.2d 540 (1963).

[241] Id. at 698, 133 S.E.2d at 544. See also Virginia v. American Booksellers Assn., 484 U.S. 383, 392-93 (1998) (permitting third-party standing in First Amendment free speech context because of potential chilling effect of law on others).

[242] In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. at 31-32, 2000 Va. Cir. LEXIS 220 at **13-**14.

[243] Id.

[244] Id., quoting in part from NAACP v. Alabama, 357 U.S. at 459.

E. Use of Special Commissioners

The Study Resolution suggested consideration of whether it would be feasible and appropriate to provide circuit court judges with "the authority to appoint special commissioners to hear and resolve complex disputes regarding the discovery of electronic data." To date, the disputes over confidentiality of the identifying information related to anonymous Internet communications has not generated a volume of motions sufficient to warrant steps at this point to delegate this responsibility. Discovery motions in general are burdensome to trial judges, but the normal practice in Virginia has been to avoid delegation of those disputes to commissioners. The particular concerns of First Amendment values implicated in the anonymous communication context studied in this report counsel in favor of leaving the decisionmaking process in the hands of the circuit court judges themselves. If the volume of the motions, or the feasibility of separating out more mechanical aspects of the review process are demonstrated in future years, the General Assembly may wish at that time to re-visit the issue of using commissioners.

F. Summary of the Proposed Mechanism

The operation of the proposed enactment may be summarized in outline form as follows:

❶ **Initiation of the Subpoena.** The applicant for a subpoena seeking information calculated to identify a person communicating anonymously on the Internet or World-Wide Web, must provide to the court in Virginia (either in obtaining a court-issued subpoena or by filing immediately after promulgating an attorney-issued subpoena) *at least 30 days prior to the scheduled disclosure* a subpoena package containing the text of the subpoena itself, along with supporting information showing (i) that one or more communications that are or may be tortious or illegal have been made by the anonymous person, or that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed, (ii) that other efforts to identify the anonymous communicator have proven fruitless, (iii) that the identity of the anonymous communicator is important, *i.e.*, is centrally needed to advance the claim, relates to a core claim or defense, or is directly and materially relevant to that claim or defense, (iv) that the actionability of the communications cannot be determined while the author remains anonymous (i.e. that no motion to dismiss, motion for judgment on the pleadings, or judgment as a matter of law, demurrer or summary judgment-type motion challenging the viability of the lawsuit of the underlying plaintiff, is pending), and (v) that the persons or entities to whom the subpoena is addressed are likely to have responsive information. The applicant serves two copies of these papers upon the subpoenaed party, along with payment sufficient to cover postage for the remailing of one copy of the application within the United States, registered and with return receipt.

❷ **Transmission to the Anonymous Communicator.** Within five business days after receipt of a subpoena application calling for identifying information concerning a client,

subscriber or customer, the subpoenaed party mails one copy thereof, by registered mail, return receipt requested, to the client, subscriber or customer whose identifying information is the subject of the subpoena.

❸ **Time for Objection or Motion**. At least five business days prior to the date on which disclosure is sought under the subpoena, any interested person may file a detailed written objection, motion to quash, or motion for protective order, which may set forth any grounds for opposing the disclosure sought in the subpoena, and must address to the extent feasible (i) whether the identity of the anonymous communicator has been disclosed in any fashion, (ii) whether the subpoena fails to allow a reasonable time for compliance, (iii) whether it requires disclosure of privileged or other protected matter and no exception or waiver applies, or (iv) whether it subjects a person to undue burden.

❹ **Timing of Compliance With Subpoena.** The party to whom the subpoena is addressed may not comply with the subpoena earlier than three business days before the date on which disclosure is due, to allow the anonymous client, subscriber or customer the opportunity to object.

❺ **Stay of Compliance Pending Court Action**. If any person files an objection, motion to quash, or motion for protective order, compliance with the subpoena shall be deferred until the appropriate court rules on the obligation to comply.

Codification of the rights and procedures involved in this process is recommended.

APPENDICES

A. Related Issues Not Central to This Report
   1. Internet Trends and Developments
   2. Internet Service Provider Immunity
   3. Personal Jurisdiction in Cyberspace
   4. The Right to Privacy in Virginia – Survey of Current Law

B. America Online v. Anonymously Traded Public Co.

C. Bibliography of Relevant Materials

APPENDIX A

Related Issues Not Central to the Report

1. Internet Trends and Developments

The Internet has become a major economic force in Virginia. It is the basis for creation of many new companies in the state and it has been a key tool to increase the profitability of many existing companies in the Commonwealth. Virginia's government and industry have actively pursued a national leadership role in Internet expansion. As a result of these efforts, some have described Virginia as the "Digital Dominion," a tribute to the Commonwealth' efforts to make Virginia as closely linked to the Internet, in the public mind, as "Silicon Valley" is to the computer industry in general.

Background: Intenet-Related Activity in Virginia

Numerous commercial and non-commercial organizations directly involved with the Internet are headquartered in Virginia, or have a major presence here.

Creation of the Internet. The two organizations that played the greatest roles in the initial development of the Internet are located in Virginia: the U.S. Department of Defense and the National Science Foundation (NSF). Without the work of these two government agencies during the 1960s, 1970s, and 1980s, the Internet would not exist. The Internet was originally a network that linked the many university and industrial research groups doing work for the Defense Department. Eventually the network expanded to link a wider range of research organizations and was managed by the NSF. In recent years, with the explosion of commercial use and the increasing number of foreign Internet users, the NSF relinquished management authority over the system. Management authority for the system is currently ambiguous, but one of the leading managers of key Internet operational functions is the Internet Corporation for Assigned names and Numbers (ICANN), a non-profit corporation. One of the key functions of ICANN is to set the policies and procedures governing Internet domain name assignment and use.

Domain name registrars. The organizations that manage the assignment of the addresses used for Internet Web sites are known as, "registrars." Currently, there are several different registrars located in various parts of the world, but the Internet's first registrar was a company called Network Solutions, Inc., which is located in Virginia, and it is still the largest domain name registrar in the world.

Internet Services Providers. Many of the world's leading Internet service providers have a major presence in Virginia. Companies such as America Online ("AOL"), PSI and UUNet are examples.

Online content developers. Many different organizations now develop content made

available using the Internet. That content comes in many different forms, including images, text, video, and audio. One of the largest developers and providers of Internet content is America Online, a company headquartered in Virginia. AOL recently completed a merger with traditional media giant, Time Warner, and with that merger, the combined AOL-Time Warner will be one of the leading providers of both online and traditional media content.

Telecommunications service providers. Virginia hosts several of the world's leading telecommunications service providers. These companies play a key role in Internet use, as they provide facilities and services that are essential to enable computers to communicate with each other. Two of the leading telecommunications companies in Virginia are Worldcom and Verizon. New telecommunications companies, cable television companies, and other entities have been created to help meet the rapidly increasing demand for Internet access.

Equipment/software developers. Companies that manufacture computer, telecommunications, and consumer electronics equipment all play key roles in Internet use. Software developers are also vital to Internet applications. Companies in all of those key industries are creating presence in Virginia. Large companies, such as IBM and Oracle, and small companies such as Xybernaut are already active in Virginia. Others, such as Intel, are building a greater presence here.

Internet associations. Internet organizations located in Virginia also include associations that focus on Internet policy issues. One leading example is The Internet Society, a non-profit organization that works to perform public interest functions on behalf of Internet users around the world. Associations representing telecommunications service providers, Internet service providers, and Internet content providers can also be found in Virginia.

Recent Legislative and Executive Initiatives

Legislative Enactments. Virginia has enacted several statutes designed to support expansion of Internet use in Virginia. In 1999, seven bills comprising the "Virginia Internet Policy Act" were enacted. The state has also enacted the Uniform Computer Information Transactions Act (UCITA, Code §§ 59.1-501.1 through –509.2, which became effective July 1, 2001, and the Uniform Electronic Transactions Act (UETA), Code §§ 59.1-479 through –497 . UCITA and UETA are intended to facilitate the expansion of commercial transactions involving computer software and other forms of electronic commercial transactions.

Other legislative initiatives currently recently considered would provide a statutory framework for registration of Web site content in Virginia, a move intended to be supportive of Web developers and Web content providers in an effort to make Virginia a haven for Web content (similar to the way Delaware has created a legal climate that attracts corporations). (Virginia Web Site Protection Act, H.B. 1491, S.B. 767).

The general assembly passed legislation in 2000 relating to the privacy of personal information contained in government systems, and Internet privacy. Section 2.1-380 was amended to prescribe that "[a]ny agency maintaining an information system that includes

personal information shall: 1. Collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency; 2. Collect information to the greatest extent feasible from the data subject directly; 3. Establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls; 4. Maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject; 5. Make no dissemination to another system without (1) specifying requirements for security and usage including limitations on access thereto-, and (11) receiving reasonable assurances that those requirements and limitations will be observed. . . 6. Maintain a list of all persons or organizations having regular access to personal information in the information system; and 7. Maintain for a period of three years or until such time as the personal information is purged, whichever is shorter, a complete and accurate record, including identity and purpose, of every access to any personal information. See Appendix A to this Report for related discussion.

Use of Digital Signature. Under the current statutes, including Code § 59.1-496 and related sections, provisions exist for using an "electronic signature" to create valid contracts or other legally effective documents. Digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as "public key cryptography," which employs an algorithm using two different but mathematically related "keys;" one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form. For a complete tutorial on digital signatures, See American Bar Association Section of Science and Technology Information Security Committee Digital Signature Guidelines Tutorial, See http://wwv.abanet.org/scitech/ec/isc/dsg-tutorial.html

Administration of the Commonwealth. Virginia state government is pursuing an "eVA" initiative, which will ultimately move a substantial amount of the state government's purchasing of goods and services onto a Web-based system. Businesses seeking to sell to the state government will eventually be able to conduct their entire competitive bidding and contract performance processes through the eVA site. Electronic purchasing and procurement systems are attractive as they can reduce costs and enhance the management controls over the execution of the purchasing function. Virginia's initiative is one of the most advanced of those now being developed among the states. For more information on Virginia's "eVA" initiative, visit: http: //eVA. state.va.us

Information Delivery. The state government currently makes active use of Internet-based systems to provide information to individuals and businesses in the state. The state's Web page, provides a popular gateway (or "portal") to information about Virginia and its government. The General Assembly has an active and popular online presence. Information about Virginia's courts (opinions, dockets, etc.) can be found at the judicial Web site, and information about federal courts in Virginia is also available on the Internet. The Virginia Department of Motor Vehicles operates an award-winning Web site providing information and processing transactions (e.g., drivers license renewals). The state has created an online portal for government services and information, the Virginia Information Providers Network

(VEPNet). For more information about Virginia Government resources on the Internet visit: http: //www.state.va.us; and http://www.vipnet.org Additional state and local government services will be accessible online in the future. Current services such as the Virtual Library of Virginia, which makes the collections of many of the state's college and university libraries accessible, will expand to help citizens of Virginia to access additional information. Virginia's schools and universities will make increasing use of the Internet.

Executive Initiatives. Governor Gilmore has taken a significant personal interest in building the Digital Dominion. That effort has included an active legislative agenda, leadership in moving an increasing number of state government functions (e.g., state purchasing and procurement activities) onto the Internet, and acceptance of personal leadership roles. The Governor chaired the advisory committee created by the U.S. Congress to begin to address the issue of taxation of Internet commercial transactions, and he served as a member of a national advisory group examining potential "cyber-terrorism" threats. For more information on the Digital Domain, see: http://www.thedigitaldominion.com

Council on Technology Services. In August 1998 Virginia Governor Gilmore announced the creation of the Council on Technology Services (COTS) to develop a blueprint for state government information technology planning and decision-making. The Council, chaired by the Secretary of Technology, has 23 members. COTS is charged, among other things, with the following: Assisting in the development of a new framework for statewide information resource planning and decision-making; assisting in the development of statewide standards, where appropriate, in all facets of information technology; participating in the development of a biennial IT Plan for state government and pilot project; and assisting in the development of other statewide programs, such as training, certification and IT workforce retention/recruitment

Electronic Government Pursuant to Executive Orders Nos. 51 and 65, the Commonwealth is to make efforts in the following areas of electronic government: 1) The development and deployment of electronic government so "that citizens and businesses interact with a more streamlined, service oriented government." 2) Increase access for the citizens of Virginia to the Internet and create digital opportunities. 3) Develop policy for privacy issues and digital signatures. 4) Establish electronic procurement for the state and its agencies to fully develop the purchasing capacity of the Commonwealth of Virginia using the Internet to procure goods and services, and obtain real value and savings for the Commonwealth. 5) Use web based-technology and apply it to state government so that administrative processes can be done more efficiently and productively in such areas employee benefits administration, leave reporting, travel planning, and expense reporting.

Privacy of Social Security Numbers. Under prevailing constitutional case law, such as Greidinger v. Davis, 988 F.2d 1344 (4th Cir. 1993), dissemination of a person's Social Security account number is restricted. Disclosure of this number is no longer required for drivers' operating licenses or voter registration.

2. Internet Service Provider Immunity

In § 230 of the Communications Decency Act of 1996, 47 U.S.C. §§ 223, 230 ("CDA"), Congress clearly and unequivocally immunized computer services providers such as America Online from liability for information that originates with third parties. Thus this issue is not one that needs to be addressed in the present study.

The relevant portion of § 230 states: "*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.*"[245]

While portions of the CDA were declared unconstitutional,[246] this immunity provision was not. Thus the federal statute supplants all prior law and shields such service providers from state or federal liability.[247]

> By its plain language, § 230 creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. Specifically, § 230 precludes courts from entertaining claims that would place a computer service provider in a publisher's role. Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions -- such as deciding whether to publish, withdraw, postpone or alter content -- are barred.[248]

The Fourth Circuit, shortly after passage of this provision, rejected claims that § 230 left intact liability for interactive computer service providers who possess notice of defamatory material posted through their services.[249] The statute applies to *any* lawsuit originating after passage of the Act. The statute broadly defines "interactive computer service" as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or

---

[245] 47 U.S.C. § 230(c)(1).
[246] See ACLU v. Reno, 521 U.S. 844 (1997).
[247] Zeran v. America Online, 129 F.3d 327, 334 (4th Cir. 1997):
While Congress allowed for the enforcement of "any State law that is consistent with [§ 230]," 47 U.S.C. § 230(d)(3), it is equally plain that Congress' desire to promote unfettered speech on the Internet must supersede conflicting common law causes of action. Section 230(d)(3) continues: "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." With respect to federal-state preemption, the Court has advised: "When Congress has 'unmistakably ... ordained,' that its enactments alone are to regulate a part of commerce, state laws regulating that aspect of commerce must fall. The result is compelled whether Congress' command is explicitly stated in the statute's language or implicitly contained in its structure and purpose." Jones v. Rath Packing Co., 430 U.S. 519, 525, 51 L. Ed. 2d 604, 97 S. Ct. 1305 (1977) (citations omitted). Here, Congress' command is explicitly stated. Its exercise of its commerce power is clear and counteracts the caution counseled by the interpretive canon favoring retention of common law principles.
[248] Zeran, 129 F.3d at 330 (Plaintiff sued the service provider, charging unreasonably delay in removing defamatory messages posted by an unidentified third party, refusal to post retractions of those messages, and failure to screen for similar postings thereafter).
[249] Id. at 332.

educational institutions."[250] The term "information content provider" is defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet or any other interactive computer service."[251] As a result, essentially all providers of such services will fall within the CDA's definition of immune "interactive computer service," and any unidentified third party who posts the offensive messages will fit the definition of an "information content provider" under the Act.

The purpose of this statutory immunity is to facilitate robust freedom for Internet communications:[252]

> The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.[253]

Numerous state and federal courts that have addressed online-related tort claims have held that Internet service providers are immune from defamation claims arising from third-party content. Moreover, it appears that the § 230 immunity generally covers all tort claims originating from third-party content, not solely defamation or defamation-like causes of action. The underlying rationale in these cases appears to be that a plaintiff cannot place an Internet service provider in the legal shoes of a subscriber (i.e., make the service provider a "speaker" or "publisher" of subscriber content) without violating § 230.[254] Other decisions have found the immunity to

---

[250] 47 U.S.C. § 230(e)(2).

[251] Id., § 230(e)(3).

[252] See Zeran, 129 F.3d at 331:
Congress recognized the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium. The imposition of tort liability on service providers for the communications of others represented, for Congress, simply another form of intrusive government regulation of speech. Section 230 was enacted, in part, to maintain the robust nature of Internet communication and, accordingly, to keep government interference in the medium to a minimum. In specific statutory findings, Congress recognized the Internet and interactive computer services as offering "a forum for a true diversity of political discourse, unique opportunities for cultural development, and myriad avenues for intellectual activity." Id. § 230(a)(3). It also found that the Internet and interactive computer services "have flourished, to the benefit of all Americans, with a minimum of government regulation." Id. § 230(a)(4) (emphasis added). Congress further stated that it is "the policy of the United States ... to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation." Id. § 230(b)(2) (emphasis added).

[253] Id.

[254] See Jonathan A. Friedman and Francis M. Buono, Limiting Tort Liability for Online Third-party Content Under Section 230 of the Communications Act, 52 Fed. Comm. L.J. 647, 657 (2000)("Friedman and Buono"). See, e.g., Doe v. America Online, Inc., 718 So.2d 385 (Fla. Dist. Ct. App. 1998) (plaintiff sued AOL under various state antipornography statutes for allowing one of its subscribers to sell, on AOL's chat rooms, pictures and videotapes of sexual acts involving the subscriber, the plaintiff, and two other minor males. The state court concluded that AOL could not be liable "as a distributor of child pornography" consistent with § 230); Acquino v. Electriciti, Inc., 26 Med. L. Rep. 1032 (Cal. Super. Ct. 1997) (§ 230 barred plaintiffs' state law claims against an Internet service provider, including claims of negligence, breach of contract, and intentional infliction of emotional distress, arising from third-party postings that stated that plaintiffs were ring leaders of an international conspiracy to further ritual satanic abuse of children).

extend to claims arising from content obtained from the service provider's "partners," even though the service provider is more than a mere conduit for a user's postings in such circumstances.[255] Thus many observers have concluded that an Internet service provider may post, promote, pay for, and edit third-party content offered on its service without subjecting itself to liability.[256] The potential applications of § 230 immunity are very broad, particularly in light of the fact that so much content that appears on or is accessible through Internet service provider networks is derived from other sources.

Virginia Provision. The Virginia legislature enacted in its 2000 session a law providing that no provider or user of an interactive computer service on the Internet shall be treated as the publisher or speaker of any information provided to it by another information content provider. The Code specifies that no provider or user of an interactive computer service shall be liable for (i) any action voluntarily taken by it in good faith to restrict access to, or availability of, material that the provider or user considers to be obscene, lewd, lascivious, excessively violent, harassing, or intended to incite hatred on the basis of race, religious conviction, color, or national origin, whether or not such material is constitutionally protected, or (ii) any action taken to enable, or make available to information content providers or others, the technical means to restrict access to information provided by another information content provider. Code § 8.01-49.1.

Contractual Limits and Waivers. While the broad construction of § 230 implemented in these court decisions provides protection from liability for Internet service providers, to further limit the potential liability arising out of the operation of a chat, message board, or similar interactive service - and to maintain family-friendly environments on their networks – many service providers post and enforce terms of service that apply specifically to such features and set forth the terms for appropriate use, as well as limitations on the service provider's liability, as well as broad indemnification provisions.

Terms and conditions of use often will include "Rules of User Conduct" [257] These rules of conduct specify that the user, in utilizing the Internet service, will not engage in any behavior that is, among other things, unlawful, threatening, abusive, harassing, defamatory,

---

[255] See Blumenthal v. Drudge, 992 F. Supp. 44 (D. D.C. 1998), for example, where a federal district court held that AOL was immune from suit based on the allegedly defamatory statements of the Drudge Report, an online gossip column that AOL made available to users. See generally, Friedman and Buono, 52 Fed. Comm. L.J. at 658. Likewise, in Ben Ezra, Weinstein & Co. v. America Online, Inc., 2000 U.S. App. LEXIS 3831 (10th Cir. 2000) a federal district court dismissed a claim against AOL based on faulty stock information available on its service. Id. The court concluded that § 230 immunity applied because third-party companies, ComStock and Townsend, had provided the content to AOL. Id. The fact that AOL worked with the two companies to correct errors in the stock information did not "constitute creating or developing the information content" provided by the two companies. Id. The Tenth Circuit recently affirmed the district court's decision. Id.

[256] See, e.g., Friedman and Buono, 52 Fed. Comm. L.J. at 659.

[257] See AOL "Rules of User Conduct" at http://www.aol.com/copyright/rules.html; Yahoo "Terms of Service" at http://docs.yahoo.com/info/terms/; AT&T Web Site "Terms and Conditions" at http://www.att.com/terms/; Verizon Online "Access Agreement" at http://www.att.com/terms/; MSN "Subscription Agreement" at http://www.msn.com/help/legal/terms.htm; CompuServe "Terms" at http://www.compuserve.com/compuserve/terms.asp; Prodigy "Subscription Agreement" at http://help.prodigy.net/help/legal/member_agreement.html.

libelous, deceptive, fraudulent, invasive of another's privacy, or tortuous.[258] Further, the provider often includes a disclaimer that it does not pre-screen, monitor, or edit the content posted by users, but that it reserves the right, at its discretion, to remove any content that, in its judgment, does not comply with its rules of user conduct or is otherwise harmful, objectionable, or inaccurate. Additionally, the provider will include a provision that it is not responsible for any failure or delay in removing such content.[259]

In addition, providers will often, in their terms of service, include limitation of liability, indemnification and termination provisions.[260]

Internet Service Providers generally also specify their privacy terms in "Privacy Policies".[261] While they indicate a strong commitment to the protection of user privacy in these policies, they also make clear the circumstances under which they will disclose information about a user. In addition, America Online has a Civil Subpoena Policy[262](a portion of the Terms of Service) in which it indicates that it will release account information or information sufficient to identify a member "only to comply with valid legal process such as a search warrant, subpoena or court order, or in special cases such as a physical threat to you or others."[263] Microsoft Network's Privacy Policy includes more broad provisions for release of user information.[264] InfoSpace has similar disclosure provisions.[265]

---

[258] Id.

[259] Id.

[260] See AOL "Member Agreement" at http://legal.web.aol.com/aolpol/memagree.html , its "Community Guidelines" at http://legal.web.aol.com/aolpol/comguide.html and its privacy policy at http://legal.web.aol.com/aolpol/privpol.html . The entire Terms of Service are also available at Keyword: TOS on the AOL service.

Limitation of Liability provision:

Under no circumstances shall America Online, its subsidiaries, or its licensors be liable for any direct, indirect, punitive, incidental, special, or consequential damages that result from the use of, or inability to use, this site. This limitation applies whether the alleged liability is based on contract, tort, negligence, strict liability, or any other basis, even if America Online has been advised of the possibility of such damage. Because some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, America Online's liability in such jurisdictions shall be limited to the extent permitted by law;

AOL Indemnification provision:

Upon a request by America Online, you agree to defend, indemnify, and hold harmless America Online and its subsidiary and other affiliated companies, and their employees, contractors, officers, and directors from all liabilities, claims, and expenses, including attorney's fees, that arise from your use or misuse of this site. America Online reserves the right, at it own expense, to assume the exclusive defense and control of any matter otherwise subject to indemnification by you, in which event you will cooperate with America Online in asserting any available defenses;

AOL Termination provision:

America Online reserves the right, in its sole discretion, to terminate your access to all or part of this site, with or without notice.

[261] See AOL Privacy Policy at http://legal.web.aol.com/aol/aolpol/privpol.html; Yahoo Privacy Policy at http://privacy.yahoo.com/privacy/us/; AT&T Privacy Policy at http://www.att.com/privacy/; Verizon Privacy Policy at http://www.verizon.net/policy/privacy.html; MSN Privacy Policy at http://www.msn.com/help/legal/privacy.htm; CompuServe Privacy Policy at http://www.compuserve.com/compuserve/privacy.asp; Prodigy Privacy Policy at http://help.prodigy.net/help/legal/privacy.html.

[262] AOL Civil Subpoena Policy at http://legal.web.aol.com/aol/aolpol/civilsubpoena.html.

[263] AOL Privacy Policy, http://legal.web.aol.com/aolpol/privpol.html .

[264] MSN Privacy Policy at http://www.msn.com/help/legal/MSNIA:

These "terms of service" and "privacy policies" are designed to provide notice to subscribers and protection to providers. Proponents of a contract approach to the Internet services market privacy regulation argue that these terms and policies are adequate. And it is true that if such "conditions of service" amount to a waiver of constitutional protections that might otherwise be available, a knowing and intelligent waiver of even important Constitutional rights is enforceable.[266] Subscribers however, may have a reasonable expectation of privacy in their Internet communications, in spite of the provisions of their user contracts, or may argue that the notice provisions in these terms are inadequate.

3. Personal Jurisdiction in Cyberspace

Because of the scope of the Internet's reach, complex personal jurisdiction issues arise with some frequency, and courts around the Nation often must determine whether they may constitutionally assert personal jurisdiction over non-resident defendants, whose only contacts with a forum are electronic. In Virginia, the "Long-Arm statute"[267] was interpreted in a landmark decision several years ago to permit assertion of jurisdiction in Virginia over a non-resident tortfeasor who completed his tortious conduct by posting a disparaging electronic message onto a computer bulletin board maintained in Virginia by a labor organization.[268] Since that time, the statute has not been amended in any respect pertinent to these issues, and no further Supreme Court decisions have dealt personal jurisdictional challenges where the in-state contact was comprised of electronic communications. Trial courts in Virginia have issued a series of disparate opinions in a variety of factual contexts, upholding or rejecting jurisdiction over non-resident defendants.[269]

The Study Resolution addressed in the present report does not focus on the issue of personal jurisdiction over non-resident defendants. Since existing law has not generated any

---

MSN Web sites will disclose your personal information, without notice, only if required to do so by law or in the good faith belief that such action is necessary to: (a) conform to the edicts of the law or comply with legal process served on Microsoft or the site; (b) protect and defend the rights or property of Microsoft, an MSN Web site; and, (c) act under exigent circumstances to protect the personal safety of users of Microsoft, its web sites, or the public.

[265] InfoSpace Privacy Policy at http://www.infospace.com/_1_4IIWU8I024553B9__info/about/truste.htm. InfoSpace may disclose personal information if required to do so by law or in the good-faith belief that such action is necessary to (a) conform to the edicts of the law or comply with legal process served on InfoSpace; (b) protect and defend the rights or property of InfoSpace, the site or the users of InfoSpace, and (c) act under exigent circumstances to protect the personal safety of users of InfoSpace, the site or the public

[266] See, e.g., Williams v. Kendrick, 184 Va. 1076, 1081, 37 S.E.2d 8, **10 (1946).

[267] Code § 8.01-328.1.

[268] Krantz v. Air Line Pilots Assoc., Int'l, 245 Va. 202, 427 S.E.2d 326 (1993)

[269] See Kent Sinclair, Personal Jurisdiction and the Internet: Courts Hold Virginia Long Arm Statute and Due Process Clause are Not Coextensive, 1999 Advance Court Rules and Pract. Serv. 3 (1999). Comparing Virginia trial court decisions such as Melvin v. Doe, 1999 WL 551335 (Loudoun County) (finding that allegations that may satisfy the Long-Arm statute were insufficient to satisfy the Due Process clause) with several federal district court and Fourth Circuit cases, including Rannoch Inc. v. The Rannoch Corp., 1999 U.S. Dist. LEXIS 10063 (E.D. Va. 1999); Bochan v. La Fontaine, 1999 U.S. Dist. LEXIS 8253 (E.D. Va. 1999) and a half-dozen cases from other federal courts.

large volume of unresolved legal issues,[270] and existing law protects Virginia citizens who believe that they have been victimized by allowing for assertion of jurisdiction to the full extent permitted by the Due Process clause,[271] any modification of the Long-Arm statute would face the risk that protections for resident plaintiffs might be diminished rather than improved by any alteration in the legal landscape.

Numerous recent publications summarize a wide range of considerations with respect to jurisdiction over alleged cyberspace tortfeasors, and the present report will simply refer the interested reader to these compendiums of cases and logical conundrums.[272]

4. The Right to Privacy in Virginia – Survey of Current Law

Unauthorized Use of Name Or Likeness. Code § 8.01-40(A) provides that if a person's "name, portrait, or picture" is used for "advertising purposes or for the purposes of trade"

---

[270] It can be argued that the trial court decision in Melvin v. Doe, 1999 WL 551335 (Loudoun County) is not wholly consistent with the Supreme Court's finding in *Krantz* that assertion of personal jurisdiction over a non-resident arising out of a single, defamatory electronic communication satisfied Due Process concerns. A single, unappealed trial court decision, however, does not suggest any lack of clarity – or substantive need for change in the approach announced by the Supreme Court in its published decision in *Krantz*.

[271] Krantz, 245 Va. at 206, 427 S.E.2d at 328.

[272] For discussions on the issue of personal jurisdiction in cyberspace, see David Bender, Emerging Personal Jurisdictional Issues on the Internet, in PLI's Second Annual Institute for Intellectual Property Law at 7, 10 (PLI Pat., Trademarks, and Literary Prop. Course Handbook Series No. 453, 1996) (discussing the issue of the extent a web site operator in one state or forum submits itself to the jurisdiction of another state or forum by the establishment of the site and allowing access to it); Susan Nauss Exon, Article: A New Shoe is Needed to Walk Through Cyberspace Jurisdiction, 11 Alb. L. J. Sci. & Tech. 1 (2000) (examining the development of personal jurisdiction from the traditional notions of contemporary standards to recent court analyses in the context of the Internet, and proposing two alternative solutions to help solve the expanding shoe size: first, a conservative solution of registration whereby potential liability can be determined within existing court systems, and second, a revolutionary shift into a new cybercourt that also involves registration); Richard S. Zembek, Comment, Jurisdiction and the Internet: Fundamental Fairness in the Networked World of Cyberspace, 6 Alb. L. J. Sci. & Tech. 339, 367 (1996) (tracing the traditional concepts of jurisdiction into the new computer medium and arguing that the existing rules and norms can be adapted to deal with the issues that arise when a non-resident defendant's contacts with a forum state are simply electronic travels or communications in the medium of cyberspace); Katherine Neikirk, Note: Squeezing Cyberspace into International Shoe: When Should Courts Exercise Personal Jurisdiction Over Noncommercial Online Speech?, 45 Vill. L. Rev. 353 (2000) (discussing the process of applying traditional personal jurisdiction principles to the Internet); Christopher McWhinney, Article: The "Sliding Scale" of Personal Jurisdiction Via the Internet, 2000 Stan. Tech. L. Rev. 1 (2000) (describing a three-category spectrum of Internet activity and a sliding-scale approach to minimum contacts analysis); Ryan Thomas, Note: Roche v. Worldwide Media, Inc.: Evaluating Where Minimum Contacts Meets Cyberspace, 31 Golden Gate U.L. Rev 293 (2001) (describing a "sliding scale" test to determine whether the exercise of personal jurisdiction based on the operation of an Internet web site alone is consistent with due process and examining the element of the intent of an Internet web site that is not captured by the quality and quantity analysis of the "sliding scale" test); Christine Heslinga, Note: The Founders Go On-Line: An Original Intent Solution to a Jurisdictional Dilemma, 9 Wm. & Mary Bill of Rts. J. 247 (2000) (suggesting that the original intent of diversity jurisdiction does not support jurisdiction in federal court for Internet diversity cases); Nicholas R. Spampata, Note: King Pennoyer Dethroned: A Policy-Analysis-Influenced Study of the Limits of Pennoyer v. Neff in the Jurisdictional Environment of the Internet, 85 Cornell L. Rev. 1742 (2000) (proposing replacing the judicially developed law of amenability with a federal amenability statute specifically drafted to satisfy efficiency and fairness concerns).

without written consent, the person may maintain a suit in equity to prevent the use, and may sue and recover damages for any injuries resulting from such use.

The Supreme Court applied § 8.01-40(A) in *Town & Country Properties* on facts involving unauthorized advertising use of the name of a famous athlete. Finding the use of the name strictly "promotional" the Court held that no constitutional protection for commercial speech limited the statutory protection. 249 Va. at 395, 457 S.E.2d at 363. Awards of compensatory and punitive damages were upheld. Id. at 398, 457 S.E.2d at 364. The statute also authorizes an injunction to prohibit further violations. See Code § 8.01-40(A).

Privacy Protection Act. In 1976 the General Assembly adopted the Privacy Protection Act, former Code § 2.1-377 through –386 (*see* Code § 2.2-3800 et seq.). These statutory provisions do not generally prohibit the dissemination of personal information. Instead, they require certain procedural steps to be taken in the collection, maintenance, use, and dissemination of such data.[273] It is also limited to governmental record keeping. Nonetheless the policies discussed in the preparation of this legislation, and the findings it recites, are pertinent to broader issues concerning dissemination of information, particularly using the Internet.

> In 1974, the General Assembly adopted a resolution directing the Virginia Advisory Legislative Council (VALC) to study and report upon the matter of computer privacy and security. S.J.R. 10, Acts 1974 at 1511. This study was generated by proliferation in the use of automated data processing equipment, especially the electronic computer, which has enabled government and private industry to compile detailed information on individuals in every area of personal activity. Report of the VALC to the Governor and General Assembly of Virginia, 2 House & Senate Documents, S. Doc. 27 at 3 (1976). There is widespread concern about infringement on individual privacy resulting from this capacity to collect, order, and disseminate explicit personal information. Id.
>
> Accordingly, a Computer Privacy and Security Committee of the Council studied the subject and in 1976 the VALC recommended legislation on regulation of computer privacy in the public sector only. Action on data systems' safeguards for the private sector was delayed.
>
> The VALC reported:
>
> "It is the intent of the Council that affirmative steps be taken now by the General Assembly to obviate the possibility of the emergence of cradle-to-grave, detailed dossiers on individuals, the existence of which dossiers would, 'at the push of a button,' lay bare to anyone's scrutiny, every detail, however intimate, of an individual's life. Such action by the General Assembly would follow in the lead of the nation's courts which have been active in developing a considerable body of case law firmly establishing privacy as an inherent, inalienable human right."

[273] See Hinderliter v. Humphries, 224 Va. 439, 297 S.E.2d 684 (1982).

Concluding its Report, the VALC said:

> In summary, the Council feels now is the appropriate time to introduce legislation to set a basis for minimum standards for personal data collection, storage, and dissemination in the Commonwealth. The General Assembly would be well advised to avoid potential gross abuse of the power of intercommunicating data banks by setting reasonable, easily implemented standards of conduct. Well managed, responsible, data systems industries and support systems are as essential to the orderly and efficient operation of modern business, industry, and government as uncontrolled, unrestricted gathering of total information dossiers about total populations are antithetical to a free society. The Council is anxious to assure the former and prevent the latter eventuality."

Subsequently, the Act was adopted by the 1976 General Assembly. Acts 1976, ch. 597. It has been said that the Act "is an important initial step towards safeguarding Virginia citizens against abusive information-gathering practices." 62 Va. L. Rev. 1357, 1358 (1976).

224 Va. at 442-443, 297 S.E.2d at 685-686.

While Virginia's Privacy Protection Act regulates only the public sector, the history of its enactment reflects the General Assembly's concern generally about the right of privacy in computer databases. The express intent to "follow in the lead of the nation's courts which have been active in developing a considerable body of case law firmly establishing privacy as an inherent, inalienable human right" indicates legislative concern beyond protection in the public sector.

In a section entitled *Findings; principles of information practice*, the Act states several important principles about the importance to individuals of privacy in the management of personal information in the computer age:

> The General Assembly finds:
>
> 1. That an individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;
>
> 2. That the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;
>
> 3. That an individual's opportunities to secure employment, insurance, credit and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems; and
>
> 4. That in order to preserve the rights guaranteed a citizen in a free

society, legislation is necessary to establish procedures to govern information systems containing records on individuals.

Former Code § 2.1-378(A). *See* Code § 2.2-3800.

A series of safeguards are called for by the Act, all directed at governmental record-keeping practices in the Commonwealth.[274] Other sections require agencies to have confidentiality controls, limit dissemination to other agencies, keep track of persons with access to information, and to record for three years "every access" to information maintained in the records. Former Code § 2.1-380 (*see* Code § 2.2-3802). No information is to be kept concerning political or religious beliefs, affiliations or activities of any person. Former Code § 2.1-380(10). *See* Code § 2.2-3803.

An Internet privacy policy is called for under the Act, such that beginning in January of 2001 government agency websites must contain a privacy policy and explanatory statement addressing "(i) what information, including personally identifiable information, will be collected, if any; (ii) whether any information will be automatically collected simply by accessing the website and, if so, what information; (iii) whether the website automatically places a computer file, commonly referred to as a "cookie," on the Internet user's computer and, if so, for what purpose; and (iv) how the collected information is being used or will be used. Former Code § 2.1-380(B).

Other provisions of the Act give certain procedural rights to persons whose information is collected. See, e.g., Former Code § 2.1-382.[275] (*See* Code § 2.2-3806). Every agency is

---

[274] B. Record-keeping agencies of the Commonwealth and political subdivisions shall adhere to the following principles of information practice to ensure safeguards for personal privacy:

1. There shall be no personal information system whose existence is secret.
2. Information shall not be collected unless the need for it has been clearly established in advance.
3. Information shall be appropriate and relevant to the purpose for which it has been collected.
4. Information shall not be obtained by fraudulent or unfair means.
5. Information shall not be used unless it is accurate and current.
6. There shall be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination.
7. There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.
8. Any agency holding personal information shall assure its reliability and take precautions to prevent its misuse.
9. There shall be a clearly prescribed procedure to prevent personal information collected for one purpose from being used for another purpose.
10. The Commonwealth or any agency or political subdivision thereof shall not collect personal information except as explicitly or implicitly authorized by law.

[275] A. Any agency maintaining personal information shall:

1. Inform an individual who is asked to supply personal information about himself whether he is legally required, or may refuse, to supply the information requested, and also of any specific consequences which are known to the agency of providing or not providing such information.
2. Give notice to a data subject of the possible dissemination of part or all of this information to another agency, nongovernmental organization or system not having regular access authority, and indicate the use for which it is intended, and the specific consequences for the individual, which are known to the agency, of providing or not providing such information, however documented permission for dissemination in the hands of such other

required to report the data collection systems it develops. Former Code § 2.1-383. *See* Code § 2.2-3807. The provisions of the Privacy Act of 1976 are not applicable to court records, publications of general circulation, juvenile and criminal justice records, professional occupation regulatory bodies, the parole board, state police, and certain other entities. See Former Code § 2.1-384. Where a violation of the principles of the Act is alleged, injunctive relief is available. Former Code § 2.1-386. *Compare* Code §§ 2.2-3802, -3809.

The legislative history of the Privacy Act clearly reflects the intent of the Virginia General Assembly to protect the "inherent, inalienable" rights of Virginia citizens in the privacy of their information system records by safeguarding against abusive information-gathering practices.

Revealing medical records in Virginia: In Virginia, there is a recognized right of privacy in the contents of a patient's medical records. Virginia Code § 32.1-127.1:03 (H)

---

agency or organization will satisfy this requirement. Such notice may be given on applications or other data collection forms prepared by data subjects.

3. Upon request and proper identification of any data subject, or of his authorized agent, grant such subject or agent the right to inspect, in a form comprehensible to such individual or agent:

(a) All personal information about that data subject except as provided in § 2.1-342 B 3.

(b) The nature of the sources of the information.

(c) The names of recipients, other than those with regular access authority, of personal information about the data subject including the identity of all persons and organizations involved and their relationship to the system when not having regular access authority, except that if the recipient has obtained the information as part of an ongoing criminal investigation such that disclosure of the investigation would jeopardize law-enforcement action, then no disclosure of such access shall be made to the data subject.

4. Comply with the following minimum conditions of disclosure to data subjects:

(a) An agency shall make disclosures to data subjects required under this chapter, during normal business hours.

(b) The disclosures to data subjects required under this chapter shall be made (i) in person, if he appears in person and furnishes proper identification, or (ii) by mail, if he has made a written request, with proper identification. Copies of the documents containing the personal information sought by a data subject shall be furnished to him or his representative at reasonable standard charges for document search and duplication.

(c) The data subject shall be permitted to be accompanied by a person or persons of his choosing, who shall furnish reasonable identification. An agency may require the data subject to furnish a written statement granting permission to the organization to discuss the individual's file in such person's presence.

5. If the data subject gives notice that he wishes to challenge, correct, or explain information about him in the information system, the following minimum procedures shall be followed:

(a) The agency maintaining the information system shall investigate, and record the current status of that personal information.

(b) If, after such investigation, such information is found to be incomplete, inaccurate, not pertinent, not timely, or not necessary to be retained, it shall be promptly corrected or purged.

(c) If the investigation does not resolve the dispute, the data subject may file a statement of not more than 200 words setting forth his position.

(d) Whenever a statement of dispute is filed, the organization maintaining the information system shall supply any previous recipient with a copy of the statement and, in any subsequent dissemination or use of the information in question, clearly note that it is disputed and supply the statement of the data subject along with the information.

(e) The agency maintaining the information system shall clearly and conspicuously disclose to the data subject his rights to make such a request.

(f) Following any correction or purging of personal information the agency shall furnish to past recipients notification that the item has been purged or corrected whose receipt shall be acknowledged.

provides that when medical records of a pro se party or a nonparty witness are subpoenaed, a statement must be issued informing the pro se party or nonparty witness of his rights and remedies. The situation is analogous to that in which a subpoena is directed to an Internet service provider for information identifying a subscriber who communicates anonymously on the Internet. Both situations involve a subpoena for disclosure of information in the setting of a recognized right of non-disclosure. In both situations, the records subpoenaed are in the custody of a third party (health care provider or Internet service provider). And in both situations, the individual whose records are requested will often not be represented by counsel and thus, without proper notice, may not otherwise be made aware of the issuance of the subpoena and the right to object to it.

Code § 32.1-127.1:03 (H) requires that notice, with specific language, in a specific format, be given to a pro se party or nonparty witness informing him that his records have been subpoenaed and that his health care provider is required to respond by disclosing those records. The following language is also required in such notice:

> If you believe your records should not be disclosed and object to their disclosure, you have the right to file a motion with the clerk of the court to quash the subpoena ...
>
> If you elect to file a motion to quash, you must notify your doctor or other health care provider(s) that you are filing the motion so that the provider knows to send the records to the clerk of court in a sealed envelope or package for safekeeping while your motion is decided.

Code § 32.1-127.1:03 (H) (1).

Notice must also be given to the health care provider as to how the records are to be handled. The provider is given notice that it is not to produce the records until ten days after the date on which the subpoena is served. Code § 32.1-127.1:03 (H) (4). This allows time for the health care provider to receive notice of the filing of a motion to quash.

Code § 32.1-127.1:03 (H) (4) further provides that in the event that the individual whose records are being sought files a motion to quash the subpoena, the court shall decide whether "good cause" has been shown by the discovering party to compel disclosure of the patient's private records over the patient's objections. The Code section goes on to specify that "in determining whether good cause has been shown, the court shall consider (i) the particular purpose for which the information was collected; (ii) the degree to which the disclosure of the records would embarrass, injure, or invade the privacy of the individual; (iii) the effect of the disclosure on the individual's future health care; (iv) the importance of the information to the lawsuit or proceeding; and (v) any other relevant factors."

Similarly, when information is subpoenaed regarding the identity of an otherwise anonymous subscriber of an Internet service provider, the subscriber should be given notice of the subpoena, information about the right to object to the subpoena, and an opportunity to file an objection before the information is disclosed. And as with the disclosure of medical records,

when an objection is made, the court should weigh the importance of the information to the underlying lawsuit against the subscriber's right to keep the information confidential.

APPENDIX B

America Online v. Anonymously Traded Public Co.

In one of the most unusual litigations to reach the Supreme Court of Virginia in some time, *America Online, Inc. v. Anonymous Publicly Traded Company*,[276] the Virginia Supreme Court addressed not only the specific issues with respect to discovery in Virginia ancillary to pending proceedings in another state, but also the general approach to be taken in determining whether a plaintiff may proceed in a "John Doe" format to preserve important privacy interests that might be affected by naming him or her on the face of the pleadings. "John Doe" pleadings have been used in Virginia in cases involving sexual abuse of minors, and other topics where confidentiality was deemed important. The new ruling will govern availability of such pleadings in the future.

The context for the important rulings was set when a publicly traded company headquartered in Indiana anonymously sued five unknown defendants in an Indiana court, alleging that the company had been defamed and was suffering the revelation of confidential information on the internet. The Indiana plaintiff sought assistance from the Virginia trial court under the Virginia Uniform Foreign Depositions Act, Va. Code Ann. § 8.01-411, to obtain discovery from AOL, a large provider of internet services, to learn the defendants' identities.

After a very scholarly consideration of the issues by Judge Stanley Klein in the Circuit Court of Fairfax County, the Supreme Court considered the general issues involved in deciding whether an anonymous litigant may utilize the coercive powers of Virginia courts under the Virginia Uniform Foreign Depositions Act, Code § 8.01-411 et seq. ("UFDA").

Pursuant to Rules 4:1(c) and 4:9(c), AOL sought to quash a subpoena duces tecum issued to it by the clerk of the circuit court and sought a protective order barring the discovery sought by an anonymous litigant proceeding as "Anonymous Publicly Traded Company" ("APTC"). The Virginia trial court refused to quash the subpoena duces tecum or issue a protective order.

The litigation has revealed that APTC is a publicly traded Delaware corporation with its principal place of business in Indianapolis, Indiana. APTC filed a complaint, captioned "Anonymous Publicly Traded Company v. John Does 1 through 5,"[277] in the Indiana court. In its complaint, APTC asserted that the John Doe defendants, whose identities and residences were unknown, "made defamatory and disparaging material misrepresentations" about APTC in internet chat rooms.[278] Additionally, APTC asserted its belief that the defendants were current and/or former employees who breached their fiduciary duties and contractual obligations by

[276] 261 Va. 350, 542 S.E.2d 377 (2001).

[277] One unusual aspect of this litigation, therefore, is that not only was the plaintiff proceeding anonymously, but the defendants' true identities were also unknown to plaintiff at the outset of this action.

[278] The Supreme Court noted in AOL that APTC defined an internet chat room as "a virtual room on the Internet where a conversation session takes place between individuals who often use pseudonyms to maintain anonymity."

publishing "confidential material insider information" about APTC on the internet. Although it did not specify what harm would be incurred by identifying itself in the Indiana court, APTC contended that it had to proceed anonymously "because disclosure of its true company name will cause it irreparable harm."

After the Indiana court issued an order permitting APTC to "proceed with a non-party production request to America Online, Inc. by obtaining a Subpoena Duces Tecum from the Virginia trial courts having jurisdiction over America Online, Inc.," the plaintiff company sought to obtain from AOL, the names, addresses, telephone numbers, and any other identifying information pertaining to four particular AOL subscribers. In granting the request, the Indiana court stated that Indiana would provide like assistance to a Virginia court or litigants, and hence notions of "comity" support the request for judicial assistance in support of the Indiana litigation.

Shortly thereafter, the Clerk of the Circuit Court of Fairfax County issued a subpoena duces tecum to AOL, requesting the names, addresses, telephone numbers, and all other identifying information regarding the four AOL subscribers. AOL indicated to APTC its intention to contest the issuance of the subpoena duces tecum in part because of the anonymity of APTC. Thereafter, APTC filed a motion in the Indiana court on October 14, 1999, for permission to proceed anonymously until it could amend its complaint to specifically name the John Doe defendants.

AOL filed its motion to quash in the Virginia trial court, arguing that APTC should not be permitted to proceed until it revealed its identity. Within a short time, however, the Indiana court issued an order granting APTC's motion to proceed anonymously. The Indiana court stated that APTC:

> Shall be allowed to proceed as anonymous in this action up and until it determines the identity of the Defendants and further determines whether to proceed with this action against the named Defendants at which time should it determine to proceed and file an amended complaint, in the amended complaint [APTC] shall list itself by its proper legal name and list those Defendants against whom it is proceeding by proper legal name.

The Indiana court did not conduct an evidentiary hearing and no reasons were given for its decision, which was rendered ex parte.

After an in camera examination of copies of the internet postings that were the subject of the underlying litigation in Indiana, the Virginia trial court issued an extensive opinion and order denying AOL's motion to quash and request for a protective order. Although the trial court conceded that there is a First Amendment interest in ensuring that courts remain open to the public, it nevertheless ruled that APTC should be permitted to proceed anonymously. Specifically, the court stated:

> As any First Amendment right of the public to know the identity of the plaintiff in the Indiana proceedings will only be marginally affected at these preliminary stages

> of those proceedings, this Court believes that comity should be accorded to the Indiana court's decision, under its Trial Rules, to allow APTC to proceed anonymously for a limited period of time. Although the Indiana court did not have the benefit of a brief from AOL when it authorized APTC to maintain its anonymity after AOL filed the instant motion, counsel herein agree that the Indiana court was then aware of AOL's objection. In addition, at least part of the salutary prophylactic effect of requiring openness in judicial proceedings has been assured by the Court's requirement that APTC supply copies of the relevant Internet postings to opposing counsel and to the Court. Both this Court and the John Does now either know or can readily ascertain the true identity of APTC. Consequently, any possible abuses of the judicial system by APTC in initiating either the proceeding in the Indiana court or in this Court can be addressed by the respective courts under applicable statutes authorizing sanctions. Hence, this Court defers, in its analysis of the issues before this Court, to the Indiana court's determination to allow APTC to maintain its anonymity for a limited period of time.

AOL appealed.

Appellate Review. Initially, the Supreme Court noted that, ordinarily, a trial court's discovery orders are not subject to review on direct appeal because they are not final within the contemplation of Code § 8.01-670. However, an order granting or refusing a motion to quash or issue a protective order, in a proceeding brought in a court of this Commonwealth pursuant to the UFDA, is a final order subject to appellate review.

The Court summarized familiar principles: The original and appellate jurisdiction of the Supreme Court of Virginia is conferred by Article VI, § 1 of the Constitution of Virginia which provides in part that, subject to constitutional limitations, "the General Assembly shall have the power to determine the original and appellate jurisdiction of the courts of the Commonwealth." The UFDA does not provide for appeal of orders pursuant to its provisions; consequently, we must look to Code § 8.01-670 for the source of the Court's appellate jurisdiction in this matter. Because this matter arises on the law side rather than the chancery side of the Circuit Court, the Court's authority to review the order of the trial court is found in Code § 8.01-670(A) which enumerates particular matters which may be the subject of appeal and concludes with subsection (3) which provides appellate jurisdiction over any matter where a "person" is "aggrieved . . . by a final judgment in any other civil case."

However, an action under the UFDA is a separate action, distinct from, although ancillary to, the underlying cause of action in the foreign jurisdiction. In the present case, therefore, when the trial court rendered its order, it disposed of every aspect of the case before it and settled all issues raised by the parties. Given the language of the UFDA, the resolution of the discovery dispute was a final, appealable judgment. The logic behind this outcome is clear:

> To hold that such an order is interlocutory and non-appealable would forever foreclose review by the orderly process of appeal and would relegate the parties to an extraordinary proceeding. Obviously, the order cannot be reviewed by this court as part of an appeal from a final judgment of the [foreign] court and cannot be reviewed by the

> [foreign] appellate court under any circumstances. Thus, although the order [**382] may have an interlocutory relationship with the [foreign] suit, we conclude that it is a final judgment on all issues in controversy in Texas and that we have jurisdiction to review it by appeal.[279]

Thus, agreeing with other states that have considered the matter under the Uniform Act, the Virginia Supreme Court held that under the UFDA an order of the trial court disposing of all issues before it and concluding the entirety of the proceedings in a Virginia court, is a final order subject to appeal under Code § 8.01-670. Discovery orders in suits brought in Virginia are interlocutory and not subject to immediate appeal. Such orders are subject to appellate review at the conclusion of the underlying suit.

The Uniform Statute. Virginia has adopted the UFDA, which provides in part:

> Whenever any mandate, writ or commission is issued out of any court of record in any other state, territory, district or foreign jurisdiction, or whenever upon notice or agreement it is required to take the testimony of a witness or witnesses or produce or inspect designated documents in this Commonwealth, witnesses may be compelled to appear and testify and to produce and permit inspection or copying of documents in the same manner and by the same process and proceeding as may be employed for the purpose of taking testimony or producing documents in proceedings pending in this Commonwealth.

Code § 8.01-411. The Supreme Court noted in *AOL* that this legislative provision is rooted in principles of comity and provides a mechanism for discovery of evidence in aid of actions pending in foreign jurisdictions. Some states have adopted the UFDA while others have adopted the Uniform Interstate and International Procedure Act. Additionally, some states have modeled their rules of civil procedure after the Federal Rules and still others have crafted their own unique rules concerning discovery proceedings in aid of foreign litigation.

Under the UFDA, reciprocity is required, and the "privilege extended to persons in other states by § 8.01-411 shall only apply to those states which extended the same privilege to persons in this Commonwealth." Code § 8.01-412.
The Supreme Court had previously recognized reciprocity with the state of Indiana based upon the UFDA.[280]

Comity Analysis. The initial question in *AOL* was whether the trial court erred in finding that the UFDA and principles of comity permit APTC to utilize the coercive power of Virginia courts while remaining anonymous. The Virginia Supreme Court, while stating " no reluctance to show due deference to the orders of the Indiana courts on any occasion when the circumstances are proper for the application of the principles of comity," concluded that the present case was not such an occasion. While it praised the Virginia trial judge's careful review

---

[279] See Warford v. Childers, 642 S.W.2d 63, 66 (Tex. Ct. App. 1982). See also, Lougee v. Grinnell, 216 Conn. 483, 582 A.2d 456 (Conn.1990), overruled on other grounds by State v. Salmon, 250 Conn. 147, 735 A.2d 333 (Conn. 1999).
[280] See Smith v. Givens, 223 Va. 455, 460, 290 S.E.2d 844, 847 (1982).

of the record, and his in camera inspection of the communications, the Court concluded that on the issue of comity, the trial court deferred to the Indiana court's determination to permit APTC to proceed anonymously for a "limited period of time" and denied AOL's motion to quash and for a protective order.

It has been held that Virginia courts should grant comity to any order of a foreign court of competent jurisdiction, entered in accordance with the procedural and substantive law prevailing in its judicatory domain, when that law, in terms of moral standards, societal values, personal rights, and public policy, is reasonably comparable to that of Virginia.[281] However, comity is not a matter of obligation. It is a matter of favor or courtesy, based on justice and good will. It is permitted from mutual interest and convenience, from a sense of the inconvenience which would otherwise result, and from moral necessity to do justice in order that justice may be done in return. Comity is not given effect when to do so would prejudice a State's own rights or the rights of its citizens.[282]

Thus the Supreme Court, while "fully appreciating the importance of comity as a guiding principle in the relationship between sovereigns and as a tool of judicial economy," noted that there are recognized limitations upon its application. Before according the privilege of comity, a showing of personal and subject matter jurisdiction has been required,[283] that "the procedural and substantive law applied by the foreign court [was] reasonably comparable to that of Virginia," id., that the decree was not "falsely or fraudulently obtained,"[284] that the order sought to be enforced was not "contrary to the morals or public policy of this State," id., and that the enforcement of the order would not "prejudice [Virginia's] own rights or the rights of its citizens."[285]

With that background the Court concluded that the action filed in Indiana is unique. The plaintiff is anonymous, as are all five John Doe defendants. Although the pleading certainly invokes the subject matter jurisdiction of the Indiana court, it is uncertain whether personal jurisdiction may be obtained over any of the anonymous defendants. Further, while the Indiana court permitted APTC to proceed anonymously, it is clear that no hearing was held concerning the question, no evidence was received by the court, no reasons for the decision were given, and the order permitting anonymous maintenance of the action was granted in a non-adversarial, ex parte proceeding. Significantly, because no evidence was received and no reasons for the decision were given by the Indiana court, we cannot determine whether the procedural and substantive law applied by the Indiana court was "reasonably comparable to that of Virginia."[286] Accordingly, the Court found that these circumstances do not present a situation where comity should be granted to the Indiana court's order permitting APTC to proceed anonymously.

---

[281] Oehl v. Oehl, 221 Va. 618, 623, 272 S.E.2d 441, 444 (1980).
[282] McFarland v. McFarland, 179 Va. 418, 430, 19 S.E.2d 77, 83 (1942).
[283] Oehl, 221 Va. at 623, 272 S.E.2d at 444.
[284] McFarland, 179 Va. at 430, 19 S.E.2d at 83.
[285] Eastern Indem. Co. v. Hirschler, Fleischer, Weinberg, Cox & Allen, 235 Va. 9, 15, 366 S.E.2d 53, 56 (1988) (citations omitted).
[286] See Oehl, 221 Va. at 623, 272 S.E.2d at 444.

Virginia Anonymity Standards. The Supreme Court held in *AOL* that wholly apart from the question of comity, a Virginia trial court may conduct an independent inquiry concerning anonymous maintenance of an action.

The Court observed that there are many reported cases in Virginia wherein a plaintiff proceeded anonymously, the issue of anonymity was resolved by consent and never presented to this Court.[287] Accordingly, the Court took the occasion to consider the circumstances under which a plaintiff may proceed anonymously in Virginia courts. A starting point is the constitutional openness of court proceedings. The Supreme Court commented that over half a century has passed since the United States Supreme Court noted, "[a] trial is a public event. . . . There is no special perquisite of the judiciary which enables it, as distinguished from other institutions of democratic government, to suppress, edit, or censor events which transpire in proceedings before it."[288] However, "the equation linking the public's right to attend trials and the public's right to know the identity of the parties is not perfectly symmetrical."[289] Accordingly, there is no absolute bar to a plaintiff proceeding anonymously. In exceptional cases, "the need for party anonymity overwhelms the presumption of disclosure mandated by procedural custom."[290]

The Court commented that upon proper circumstances, courts must balance the need for anonymity against the general presumption that parties' identities are public information and the risk of unfairness to the opposing party.[291] As the Eleventh Circuit has stated, "the ultimate test for permitting a plaintiff to proceed anonymously is whether the plaintiff has a substantial privacy right which outweighs the customary and constitutionally-embedded presumption of openness in judicial proceedings. It is the exceptional case in which a plaintiff may proceed under a fictitious name."[292]

In a review of decisions from throughout the country, the Fourth Circuit compiled a list of "factors that should be considered by courts considering anonymity requests."[293] Such factors included:

> Whether the justification asserted by the requesting party is merely to avoid the annoyance and criticism that may attend any litigation or is to preserve privacy in a matter of sensitive and highly personal nature; whether identification poses a risk of retaliatory physical or mental harm to the requesting party or even more critically, to innocent non-parties; the ages of the persons whose privacy interests are sought to be protected; whether the action is against a governmental or private party; and, relatedly,

---

[287] The Court mentioned A.H. v. Rockingham Publ'g Co., 255 Va. 216, 219 n.2, 495 S.E.2d 482, 484 n.2 (1998), where it was noted that "because this claim arises out of a sexual assault on a minor, the plaintiff used a pseudonym to protect his identity." See also Doe v. Doe, 222 Va. 736, 284 S.E.2d 799 (1981); Baby Doe v. John and Mary Doe, 15 Va. App. 242, 421 S.E.2d 913 (1992); C.P. v. Rockingham Publ'g Co., 34 Va. Cir. 79 (1994); Jane and John Roe v. Richmond Metro. Blood Serv., Inc., 22 Va. Cir. 111 (1990).

[288] Craig v. Harney, 331 U.S. 367, 374 (1947).

[289] Doe v. Stegall, 653 F.2d 180, 185 (5th Cir. 1981).

[290] Id.

[291] See Does I Thru XXIII v. Advanced Textile Corp., 214 F.3d 1058, 1068 (9th Cir. 2000).

[292] Doe v. Frank, 951 F.2d 320, 323 (11th Cir. 1992) (citation and internal quotation marks omitted).

[293] James v. Jacobson, 6 F.3d 233, 238 (4th Cir. 1993).

the risk of unfairness to the opposing party from allowing an action against it to proceed anonymously.

The Virginia Supreme Court noted in *AOL* that the types of cases in which plaintiffs have been permitted to proceed anonymously in other courts in the nation include birth control cases, abortion cases, welfare cases involving illegitimate children, and cases involving issues of homosexuality.[294]

Thus, the limited situations in which a plaintiff has been permitted to proceed under a pseudonym involve "the presence of some social stigma or the threat of physical harm to the plaintiffs attaching to disclosure of their identities to the public record."[295] The Court observed that a common thread throughout these decisions is that the likelihood of the plaintiff suffering some embarrassment or economic harm is not enough by itself to permit anonymity.[296]

However, the Virginia Supreme Court echoed the findings of the Ninth Circuit Court of Appeals, where the court stated that anonymity may never be used to protect against economic harm is "incorrect as a matter of law."[297] Rather, in some instances, the level of retaliation in the form of economic harm may rise to an extraordinary level permitting plaintiffs to proceed anonymously.[298]

Rule 3:3 embraces the normative principle of disclosure and requires the "names" of the parties to be stated in pleadings. However, like other courts that have considered the issue, the Virginia Supreme Court recognized that there are certain circumstances when permitting a plaintiff to proceed under a pseudonym must be entrusted to the sound discretion of the trial court. The Court stated that the factors considered by the Fourth Circuit in *James*, while not exhaustive, are appropriate for consideration by state courts in Virginia.

Accordingly, the Virginia Supreme Court concluded that "upon showing of special circumstances when a party's need for anonymity outweighs the public's interest in knowing the party's identity and outweighs the prejudice to the opposing party, a court may exercise its discretion to allow a party to proceed anonymously." The Court also commented in passing, that, of course, circumstances may change as litigation progresses, thereby requiring reconsideration of initial rulings.

In the facts of the anonymous proceeding against AOL, the sole reason that the would-be anonymous Indiana corporation had offered in support of its request to proceed anonymously was fear of economic harm. The Supreme Court said: "While reasonable concern

---

[294] See Doe v. Deschamps, 64 F.R.D. 652, 653 (D. Mont. 1974) (citing Roe v. Wade, 410 U.S. 113, 35 L. Ed. 2d 147, 93 S. Ct. 705 (1973) (abortion); Doe v. Gillman, 347 F. Supp. 483 (N.D. Iowa 1972) (child born out of wedlock); Doe v. Chafee, 355 F. Supp. 112 (N.D. Cal. 1973) (homosexuality)).

[295] Doe v. Rostker, 89 F.R.D. 158, 161 (N.D. Cal. 1981).

[296] Doe v. Goldman, 169 F.R.D. 138, 141 (D. Nev. 1996); Doe v. Hallock, 119 F.R.D. 640, 644 (S.D. Miss. 1987); Doe v. Rostker, 89 F.R.D. at 163; Doe v. Diocese Corp., 43 Conn. Supp. 152, 647 A.2d 1067, 1071 (Conn. Super. Ct. 1994); A.B.C. v. XYZ Corp. and XYZ Co., 282 N.J. Super. 494, 660 A.2d 1199, 1204 (N.J. Super. Ct. 1995).

[297] Does I Thru XXIII v. Advanced Textile Corp., 214 F.3d at 1070.

[298] 214 F.3d at 1071.

over potential economic harm is not excluded from factors to consider, APTC has not borne its burden to show special circumstances justifying anonymity."

The Virginia Supreme Court castigated the showings advanced by the anonymous litigant for the "conclusory nature" of its reasons for anonymity. Those arguments do not reveal the degree and nature of any potential economic harm. While the anonymous litigant would have the trial court trust its decision rather than submit evidence so that an independent judicial evaluation can be made concerning the need for anonymity, the Supreme Court of Virginia found this approach unacceptable.

APPENDIX C

Bibliography of Relevant Materials

1. Statutes and Rules

Virginia

- Uniform Foreign Depositions Act
  - Va. Code Ann. § 8.01-411
  - Va. Code Ann. § 8.01-412
  - Va. Code Ann. § 8.01-412.1
- Va. Code § 8.01-328.1 (personal jurisdiction)
- Va. Code Ann. § 19.2-70.3
- Virginia Supreme Court Rules 4:9(c)
- Virginia Supreme Court Rules 4:2

Federal

- Electronic Communications Privacy
  - 18 U.S.C. §2701 et seq.
- FED. R. CIV. P. 45
- FED. R. CIV. P. 27
- Communication Decency Act
  - 47 U.S.C.S § 223
  - 47 U.S.C.S. § 230
- Federal Title III Wiretap Act
  - 18 U.S.C. § 2518(3)

California

- Cal Code Civ Proc § 425.16

Georgia O.C.G.A. § 16-9-93.1 (1996) (criminalizing falsely identifying transmissions)

2. Provider Terms and Policies

AOL Civil Subpoena Policy
AOL Privacy Policy
EarthLink Service Agreement
EarthLink Privacy Policy
EarthLink Acceptable Use Policy

AT&T Terms and Conditions
AT&T Privacy Policy
Juno Service Agreement
Juno Privacy and Security
MSN Subscription Agreement
MSN Privacy Statement
Prodigy Subscription Agreement
Prodigy Privacy Policy
Verizon Access Agreement
Verizon Policy Statement
Yahoo Terms of Service
Yahoo Privacy
CompuServe Terms
CompuServe Privacy
InfoSpace Terms of Use
InfoSpace Privacy

3. Case law

Melvin v. Doe, 1999 WL 551335 (Va. Cir. Ct. June 24, 1999)

(no jurisdiction in Virginia courts over defamation action against anonymous speaker where only alleged basis for jurisdiction was AOL's presence in Virginia; quashing subpoena issued in connection with such action); (Pa. Ct. of Common Pleas Nov. 15, 2000) ("A plaintiff should not be able to use the rules of discovery to obtain the identity of an anonymous publisher simply by filing a complaint that may, on its face, be without merit.").

In re Request for Subpoena Duces Tecum to America Online, Inc., 50 Va. Cir. 202; 1999 Va. Cir. LEXIS 406 (Va. Cir. Loudoun County, August 17, 1999).

(In considering motion to quash subpoena, the court analogized to the criminal subpoena relevancy standard. It required AOL to give notice to John Does defendants, at plaintiff's expense. It also noted that the more appropriate forum for considering the First Amendment issues was the court in the underlying action.)

In re Subpoena Duces Tecum to America Online, Inc (IPA v. May, No. 107CL00022399-00 (Va. Cir. Ct. Dec. 6, 1999)

(protective order granted excusing AOL from compliance with subpoena due to plaintiff's failure to provide court with mandate, writ, or commission from court in which underlying action was pending).

In re Texaco Inc., Law No. 23163 (Va. Cir. Ct. Mar. 14, 2000)

("[A] Virginia Court does not acquire jurisdiction merely because an actionable email passed through AOL's facilities in Loudoun County, Virginia.") (use of Va. Sup. Ct. R. 4:2 to obtain discovery inappropriate).

In re Subpoena Duces Tecum to America Online, Inc. (Anonymous Publicly Traded Co. v. Does), Misc. Law No. 40570 (Va. Cir. Ct. 2000)

("[A] court should only order a non-party, Internet service provider to provide information concerning the identity of a subscriber (1) when the court is satisfied by the pleadings or evidence supplied to that court (2) that the party requesting the subpoena has a legitimate, good faith basis to contend that it may be the victim of conduct actionable in the jurisdiction where suit was filed and (3) the subpoenaed identity information is centrally needed to advance that claim.").

Global Telemedia Int'l. Inc., et al. v. Does, No. 00-1155 DOC (EEx) (C.D. Cal Feb. 23, 2001) (granting Does' motion to dismiss where court found that message board postings contained opinions rather than actionable facts).

Dendrite Int'l v. John Does (N.J. Super. Ct. Ch. Div. Nov. 23, 2000)(aff'd July 11, 2001) (adopting Seescandy.com analysis and denying request for order granting leave to conduct discovery aimed at identifying Does who opposed request).

http://legal.web.aol.com/aol/aolpol/dendrite.pdf

Aquacool_2000 v. Yahoo! Inc. Complaint

http://legal.web.aol.com/decisions/dlpriv/aquacoolcomplaint.pdf

Stone & Webster, Inc. v. John Does, No. 99MS-0713 (Franklin Cty. Ct. Feb. 7, 2000) (cited in Dendrite), the Ohio Court of Common Pleas denied a motion to quash a subpoena for identifying information, reasoning that the first Amendment protected against governmental actions rather than private conduct. Furthermore, the court reasoned that the defendant voluntarily gave his true identity to CompuServe.

McIntyre v. Ohio Elections Commission, 514 U.S. 334 (1995)

("[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.").

ACLU v. Johnson, 4 F. Supp. 2d 1029 (D.N.M. 1998), aff'd, 194 F.3d 1149 (10th Cir. 1999) (First Amendment right to anonymity applies to "communicating and accessing information anonymously" over the Internet).

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

(protected speech includes "the use of false identification to avoid social ostracism, to prevent discrimination and harassment, and to protect privacy").

Columbia Insurance Company v. Seescandy.com, 185 F.R.D. 573 (N.D. Cal. 1999) (because of the "legitimate and valuable right to participate in online forums anonymously or

pseudonymously," party seeking discovery to uncover the identity of an online speaker must satisfy a heightened burden, including establishing that suit could withstand motion to dismiss).

NLRB v. Midland Daily News, 151 F.3d 472 (6th Cir. 1998)
(party seeking identity of anonymous speaker must demonstrate a reasonable basis for seeking such information).

Rancho Publications v. Superior Court, 81 Cal. Rptr. 2d 274 (Cal. Ct. App. 1999)
("The need for discovery [of the identity of anonymous speakers] is balanced against the magnitude of the privacy invasion, and the party seeking discovery must make a higher showing of relevance and materiality than otherwise would be required for less sensitive material.").

In re 2theMart.com, 2001 U.S. Dist. LEXIS 5318 (W.D. Wash.)
Memo in support of Motion to Quash
Memo in opposition to Motion to Quash
Brief of InfoSpace, seeking balancing test

United States v. Hambrick, 55 F.Supp. 2d 504 (W.D. Va. 1999).
(finding no reasonable expectation of privacy in identity information)

Medinex v. Awe2bad4mdnx
Article re case dismissal
EFF Motion to Quash

Reno v. ACLU, 521 U.S. 844 (1997)
Invalidated some provisions of Communications Decency Act, but maintained immunity for service providers for information originating with a third party user of the service. (Injured party must therefore seek out the individual who posted the defamatory message, not the provider).

Hritz v. Doe (E.D. Va.) Public Citizen Memo Supporting MTQ

CompuServe v. Patterson, 89 F.3d 1257 (6th Cir. 1996).
(holding that defendant had sufficient contacts with forum state by purposefully availing himself of privilege of doing business in state by marketing product through state Internet service provider, supporting the exercise of personal jurisdiction.)

Telco Communications v. An Apple a Day, 977 F.Supp. 404 (E.D. Va. 1997)
Defendant's posting of a Website, which could be accessed by Virginia residents 24 hours a day, constituted a persistent course of conduct under the Virginia long-arm statute.

Rovario v. United States, 353 U.S. 53 (1957)

(Balancing test for disclosure of identity- depends on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors.

Zeran v. America On-Line, 958 F.Supp. 1124 (E.D. Va.), *aff'd* 129 F.3d 327 (1997)
Interpreting 47 U.S.C. § 230, Immunity from liability for ISPs. Case cites Cubby v. Compuserve, 776 F.Supp. 135 (S.D. N.Y. 1991); Stratton Oakmont v. Prodigy, 1995 N.Y. Misc. Lexis 229 (1995);

Talley v. California, 362 U.S. 60 (1960)
(invalidating a California statute prohibiting the distribution of handbills without identifying information.

4. Law Review Articles

Michael H. Spencer, *Anonymous Internet Communication and the First Amendment: A Crack in the Dam of National Sovereignty*, 3 Va. J.L. & Tech. 1 (1998)

David L. Sobel, *The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 Va. J.L. & Tech. 3 (2000)

A. Michael Froomkin, *Anonymity and Its Enmities,* 1995 J. Online L. art. 4 (May, 1995)

Jay Krasovec, *Cyberspace:: The Final Frontier, for Regulation?,* 31 Akron L. Rev. 101 (1997).

George H. Carr, Note*: Application of U.S. Supreme Court Doctrine To Anonymity In The Networld,* 44 Clev. St. L. Rev. 521 (1996).

Lee Tien, Symposium*: Innovation and the Information Environment: Who's Afraid of Anonymous Speech? McIntyre and the Internet,* 75 Or. L. Rev. 117 (Spring 1996)

George B. Trubow, Symposium Article*: Regulating Transactions of the Internet,* 24 Ohio N.U.L. Rev. 831 (1998)

Suman Mirmira, *Lunney v. Prodigy Services Co.,* 15 Berkeley Tech. L.J. 437 (2000).

George P. Long, III, Symposium*: Comment: Who Are You?: Identity and Anonymity in Cyberspace,* 55 U. Pitt. L. Rev. 1177 (Summer 1994)

Anne Wells Branscomb, Symposium: Emerging Media Technology and the First Amendment: Anonymity,Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces, 104 Yale L.J. 163 ((May 1995).

David R. Johnson and Kevin A. Marks, *Mapping Electronic Data Communication onto Existing Legal Metaphors: Should We Let Our Conscience (and Our Contracts) Be Our Guide?,* 38 Vill. L. Rev. 487 (1993).

Seth Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law,* 140 U. Pa. L. Rev. 1 (1991).

Noah Levine, *Note: Establishing Legal Accountability for Anonymous Communication in Cyberspace,* 96 Colum. L. Rev. 1526 (1996).

Ronald Brown, et al., *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information,* U.S. Department of Commerce (1995).