SUPREME COURT OF NEW JERSEY
DOCKET NO. 60-756

STATE OF NEW JERSEY, Plaintiff	:	Criminal Action
v.	:	On Appeal from the Superior Court,
SHIRLEY REID, Defendant	:	Appellate Division No. A-003424-08T5

BRIEF OF *AMICI CURIAE*
AMERICAN CIVIL LIBERTIES UNION OF NEW JERSEY,
ELECTRONIC FRONTIER FOUNDATION,
ELECTRONIC PRIVACY INFORMATION CENTER,
FREEDOM TO READ FOUNDATION, PRIVACY RIGHTS CLEARINGHOUSE,
AND NEW JERSEY LIBRARY ASSOCIATION

Grayson Barber, Esq.
Grayson Barber, L.L.C.
68 Locust Lane
Princeton, New Jersey 08540
(609) 921-0391

On the Brief:
Grayson Barber
Lee Tien
Ed Barocas

TABLE OF CONTENTS

STATEMENT OF INTEREST OF *AMICI CURIAE*		**1**
ARGUMENT		**4**
I.	**THE NEW JERSEY CONSTITUTION IS AN INDEPENDENT SOURCE OF PROTECTION FOR INDIVIDUAL RIGHTS**	**5**
II.	**INTERNET SUBSCRIBER RECORDS IMPLICATE SEVERAL PRIVACY AND FIRST AMENDMENT FREE SPEECH INTERESTS**	**10**
III.	**THIRD-PARTY SUBPOENAS THAT IMPINGE UPON CONSTITUTIONAL INTERESTS MERIT JUDICIAL SCRUTINY**	**30**
IV.	**THE DOUBLY DEFECCTIVE SUBPOENA FOR INFORMATION ABOUT REID VIOLATED STATE STATUTE**	**40**
CONCLUSION		

TABLE OF AUTHORITIES

Berger v. New York, 388 U.S. 41 (1967) 12

Bron v. Weintraub, 42 N.J. 87 (1964) 5

Buckley v. American Const. Law Found, 525 U.S. 182 (1999) 22

Burrows v. Superior Court, 13 Cal.3d 238 (1975) 19

Casey v. Male, 63 N.J. Super. 255 (Co. Ct. 1960) 3

Columbia Ins.Co. v. Seescandy.com, 185 F.R.D. 573 (N.D.Cal. 1999) 33

Dendrite Int'l, Inc. v. John Doe No. 3, 342 N.J. Super. 134 (App. Div. 2001) 30, 32, 33

Doe v. 2TheMart.com, 140 F.Supp.2d 1088 (W.D. Wa. 2001) 33

Doe v. Poritz, 142 N.J. 1 (1995) 11, 12, 17

Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539 (1963) 11

Greenberg v. Kimmelman, 99 N.J. 552 (1985) 11

Hennessey v. Coastal Eagle Point Oil Co., 129 N.J. 81 (1992) 9

Immunomedics v. Doe, 342 N.J. Super. 160 (App. Div. 2001) 33

In re Addonizio, 53 N.J. 107 (1968) 30

In re Grady, 85 N.J. 235 (1981) 11

In re Martin, 90 N.J. 295 (1982) 8

In re Quinlan, 70 N.J. 10 (1976) 11

Katz v. United States, 389 U.S. 347 (1967) 8

Klimas v. Comcast, 465 F.3d 271 (6th Cir. 2006) 14

Kreimer v. Morristown, 958 F.3d 1242 (3d Cir. 1992) 28

Kyllo v. United States, 533 U.S. 27 (2001) 12

McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) 20, 21

NAACP v. Alabama ex rel Patterson, 357 U.S. 449 (1958) 11

New Jersey Coalition Against War in the Middle East v. JMB Realty, 138 N.J. 326 (1994) 21

Olmstead v. United States, 277 U.S. 438 (1928) 37

Planned Parenthood v. Farmer, 165 N.J. 609 (2000) 7

Reno v. ACLU, 521 U.S. 844 (1997) 21, 23, 28

Right to Choose v. Byrne, 91 N.J. 287 (1982) 11

Shelton v. Tucker, 364 U.S. 479, 490 (1960) 11

State v. Alston, 88 N.J. 211 (1981) 7, 10

State v. Baker, 81 N.J. 99 (1979) 12

State v. Ballard, 331 N.J.Super. 529 (App. Div. 2000) 38

State v. Bruzzese, 94 N.J. 210 (1983) 9

State v. Domicz, 188 N.J. 285 (2006) 10

State v. Evers, 175 N.J. 355 (2003) 25

State v. Hempele, 120 N.J. 182 (1990) 9, 34

State v. Hunt, 91 N.J. 338 (1982) 10

State v. Johnson, 68 N.J. 349 (1975) 10

State v. McAllister, 184 N.J. 17 (2005) 10,17,19,20,31,35

State v. Mollica, 114 N.J. 329 (1989) 5, 10

State v. Novembrino, 105 N.J. 95 (1987) 6, 9

State v. Pierce, 136 N.J. 184 (1994) 9, 10

State v. Reid, 389 N.J. Super. 563 (App. Div. 2007) 40

State v. Saunders, 75 N.J. 200 (1977) 9, 11

State v. Schmid, 84 N.J. 535 (1980), *appeal dismissed, sub nom.*, Princeton University v. Schmid, 455 U.S. 100 (1982) 5

State v. Soto, 324 N.J.Super. 66 (Law Div. 1996) 38

Talley v. California, 362 U.S. 60 (1960) 21

Tattered Cover v. City of Thornton, 44 P.3d 1044 (2002) 36

Taxpayers Assoc. of Weymouth Twp. v. Weymouth Twp., 80 N.J. 6 (1976), *cert. denied*, 430 U.S. 977 (1977) 3

Warshak v. U.S., -- F.3d --, 2007 U.S.App. Lexis 14297 (6th Cir. 2007) 13, 25

Wilson v. Layne, 526 U.S. 603 (1999) 12

Zeran v. America Online, 129 F.3d 327 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998) 27

Constitution of the State New Jersey, Article I, Paragraphs 1 and 7 6

N.J.S.A. 2A:156A-29f 40, 41

N.J.S.A. 18A:73-43.1 to 18A:73-43.3 2, 28

"Bronco" a.k.a. C.R. Scott, "Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations." In S. Drucker (Ed.), 41 Free Speech Yearbook 127 (2004) 22, 23

Preston Gralla, How the Internet Works (MacMillan Computer Publishing 1999) 13

Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it, 72 Geo.Wash.L.Rev. 1208 (2004) 18

Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1598 (2004) 32

Daniel Solove, Reconstructing Electronic Surveillance Law, 72 Geo. Wash. L. Rev. 1264 (2004) 16, 17

STATEMENT OF INTEREST OF AMICUS CURIAE

Amicus curiae American Civil Liberties Union of New Jersey (ACLU-NJ) is a private non-profit, non-partisan membership organization dedicated to the principle of individual liberty embodied in the Constitution. Founded in 1960, the ACLU-NJ has approximately 14,000 members in the State of New Jersey. The ACLU-NJ is the state affiliate of the American Civil Liberties Union, which was founded in 1920 for identical purposes, and is composed of over 400,000 members nationwide.

The Electronic Frontier Foundation (EFF) is a nonprofit, membership-supported civil liberties organization working to protect civil rights and free expression in the digital world. EFF's interest in this case arises because the government's use of third-party subpoenas poses a significant threat to free and robust expression on the Internet.

The Electronic Privacy Information Center (EPIC) is a public interest research center dedicated to protecting individual privacy and bringing public attention to emerging civil liberties issues. EPIC has participated as amicus curiae in numerous privacy cases before the U.S. Supreme Court and nationwide.

The Freedom to Read Foundation is a not-for-profit organization established in 1969 by the American Library Association to promote and defend First Amendment rights, to foster libraries as institutions that fulfill the promise of the First Amendment for every citizen, to support the right of libraries to include in their collections and make available to the public any work they may legally acquire, and to establish legal precedent for the freedom to read of all citizens.

The Privacy Rights Clearinghouse (PRC) is a nonprofit consumer organization with a two-part mission -- consumer information and consumer advocacy. Based in San Diego, California, it is primarily grant-supported and serves individuals nationwide. One of PRC's primary goals is to raise awareness of how technology affects personal privacy.

The New Jersey Library Association (NJLA), established in 1890 and with current membership exceeding 1700 individuals and libraries, is the oldest and largest library association in New Jersey. NJLA is active in a variety of public policy arenas advocating for the advancement of library services in New Jersey and training its members in best practices of library administration and management. The New Jersey library confidentiality statute, N.J.S.A. 18A:73-43.1 to 43.3, requires all library staff to

ask for a "subpoena issued by a court" or a count order before disclosing patron information to any individual including law enforcement officials.

This case raises far-reaching questions about the scope of privacy protection in the electronic environment. The participation of *amici curiae* is particularly appropriate in cases with "broad implications," Taxpayers Assoc. of Weymouth Twp. v. Weymouth Twp., 80 N.J. 6, 17 (1976), *cert. denied*, 430 U.S. 977 (1977), or in cases of "general public interest." Casey v. Male, 63 N.J. Super. 255, 259 (Co. Ct. 1960) (history and parameters of *amicus curiae* participation). This is such a case.

ARGUMENT

It is without question a burden to the police that they may not freely seize evidence, intercept phone calls, or detain individuals without probable cause, but this is a burden that every constitutional democracy accepts as a fundamental requirement to safeguard the rights of its citizens. When the government obtains personal information through improper means, New Jersey courts should suppress that information in order to protect the fundamental right of privacy.

It is a fact of modern life that in the digital age, a great deal of personal communication occurs over the Internet. In addition, personal information that people used to keep in paper files or on computer hard drives is increasingly stored online, beyond the physical confines of home or office. The method required to engage in this medium inexorably involves third parties: Internet Service Providers (ISPs). Online service providers offer their customers the ability to store photos, e-mail, calendars, and documents on the Internet. Yet this fact of modern life must not be permitted to erode privacy and speech rights. Indeed, this Court had made clear that when "society becomes from time to time more complex … new

applications of old principles are required." Bron v. Weintraub, 42 N.J. 87, 93 (1964).

I. THE NEW JERSEY CONSTITUTION IS AN INDEPENDENT SOURCE OF PROTECTION FOR INDIVIDUAL RIGHTS.

A very important function of the state constitution is to protect individuals against unwarranted intrusion by the government. The constitution and laws of New Jersey provide structure to the relationships between individuals and law enforcement, maintaining an appropriate balance of power in these relationships. This Court must interpret the constitution to safeguard liberty, and to control law enforcement institutions so that they remain accountable to the people.

"It is now firmly recognized that state constitutions do not simply mirror the federal Constitution; they are a basis for independent rights and protections that are available and applicable to the citizens of the state." State v. Mollica, 114 N.J. 329, 352 (1989). This Court has repeatedly expressed the firm belief that "state constitutions exist as a cognate source of individual freedoms and that state constitutional guarantees of these rights may indeed surpass the guarantees of the federal Constitution." State v. Schmid, 84 N.J. 535, 553 (1980), *appeal dismissed sub nom.*, Princeton University v. Schmid,

455 U.S. 100 (1982). "This Court has frequently resorted to our State Constitution in order to afford our citizens broader protection of certain personal rights than that afforded by analogous or identical provisions of the federal constitution." State v. Novembrino, 105 N.J. 95, 145 (1987).

In New Jersey, the constitutional right to privacy includes a right to be free from state interference on illegitimate grounds. It is found in two paragraphs of Article I, Paragraph 1 provides that: "All persons are by nature free and independent, and have certain natural and inalienable rights, among which are those of enjoying life and liberty, of acquiring, possessing and protecting property and of pursuing and obtaining safety and happiness." Paragraph 7 provides a privacy right in the context of search and seizure: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."

As to Article I, paragraph 1, this Court has made it clear that "the language of the paragraph is more expansive than that of the U.S. Constitution. It incorporates within its terms the right of privacy and its concomitant

rights…." Planned Parenthood v. Farmer, 165 N.J. 609, 629 (2000). *See also* State v. Alston, 88 N.J. 211, 225 (1981).

Privacy involves aspects of personal life and social practices that pertain to our most basic needs and desires: family life, sexual activity, political activity, finances, employment, and free expression. Solicitous of the individual rights conferred by the state constitution, this Court has rejected the more parsimonious interpretations of federal law in the area of privacy. Id.

This right is not constrained by the "reasonable expectation of privacy" rubric of federal Fourth Amendment jurisprudence. This Court has recognized that the federal standard is vague and subject to the potential for inconsistent and capricious application. Alston, 88 N.J. at 227-228 (rejecting as "amorphous" the "legitimate expectations of privacy in the area searched" standard). Rather, the New Jersey standard provides protection beyond that, focusing on whether there is a possessory interest in the information or items being seized. Id.

Even under the less protective federal standard, however, it is a common myth that there is no "reasonable expectation of privacy" against practices that have been in place for some time or against practices that have, to some extent, occurred in public. The U.S. Supreme Court's 1967

decision in Katz v. United States, 389 U.S. 347 (1967), invalidated the kind of government wiretapping that had been commonplace since the invention of the telephone system. Moreover, Katz made his telephone call from a glass booth in downtown Los Angeles. Despite that, the Court spoke of "the privacy upon which he justifiably relied." Although "[w]hat a person *knowingly* exposes to the public … is not a subject of Fourth Amendment protection," id. at 351 (emphasis added), protection still exists for disclosures made under duress, or in circumstances understood to be confidential – as was the case here with the transmission of personal information to an ISP.

A cognizable privacy interest still exists even in very public actions, such as computer-aided transactions in open-air venues considered "public," such as ATM machines. Similarly, the secrecy of the ballot box must be preserved, notwithstanding that one must now use the process of electronic voting machines.

The privacy interest protected by the state constitution is a fundamental right. In re Martin, 90 N.J. 295, 318 (1982) (the Court must balance government's need of information against the individual's right of confidentiality). The right to privacy is one of the "natural and inalienable rights" recognized by the state

constitution. Hennessey v. Coastal Eagle Point Oil Co., 129 N.J. 81, 96 (1992). As such, governmental interference with the right can be justified only by a compelling state interest. Even if the governmental purpose is legitimate and substantial, the invasion of the fundamental right of privacy must be minimized by utilizing the narrowest means which can be designed to achieve the public purpose. State v. Saunders, 75 N.J. 200, 217 (1977).

As to Article I paragraph 7, likewise, this Court has found that the State constitution affords our citizens greater protections against unreasonable searches and seizures than does the Fourth Amendment. "We recognize that this Court has the power to afford citizens of this State greater protection against unreasonable searches and seizures than may be required by the Supreme Court's prevailing interpretation of the Fourth Amendment." State v. Bruzzese, 94 N.J. 210, 216 (1983).

In each of the following cases, this Court has held that paragraph 7 affords greater privacy protection than federal law: State v. Novembrino, *supra*, 105 N.J. at 158 (no good faith exception to the exclusionary rule); State v. Hempele, 120 N.J. 182 (1990)(garbage left at the curbside); State v. Pierce, 136 N.J. 184 (1994) (police are not authorized to search a vehicle incident to warrantless

arrest of driver for driving with suspended license); State v. Hunt, 91 N.J. 338 (1982) (phone-toll billing records); State v. Alston, 88 N.J. 211 (1981) (standing to challenge validity of searches); State v. Johnson, 68 N.J. 349 (1975) (burden to show validity of non-custodial consent to search). This "body of decisional law reflects a steadily-evolving commitment by our State courts to provide enhanced protection for our citizens against encroachment of their right to be free from unreasonable searches and seizures." Pierce, 136 N.J. at 209.

II. INTERNET SUBSCRIBER RECORDS IMPLICATE SEVERAL SIGNIFICANT PRIVACY AND FREE SPEECH INTERESTS

New Jersey courts have long recognized that the state constitution protects New Jersey residents' rights of privacy in records about them and their activities. State v. Hunt, 91 N.J. 338 (1982) (records of home telephone use); State v. Mollica, 114 N.J. 329 (1989) (records of hotel telephone use); State v. McAllister, 184 N.J. 17 (2005) (bank records); State v. Domicz, 188 N.J. 285 (2006) (utility records).

This case implicates several different privacy interests. "*Privacy of communications*" covers the security and privacy of mail, telephones, e-mail and other forms of communication. *See, e.g.*, State v. Hunt, 91 N.J. 338

(1982)(wiretaps). "*Information privacy*" pertains to the treatment of personally identifiable information. *See, e.g.*, Doe v. Poritz, 142 N.J. 1, 87 (1995). It involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. Id., 142 N.J. at 87 (home address).[1]

Communications records, and Internet records in particular, also implicate "*Associational privacy*." There is a "vital relationship between freedom to associate and privacy in one's associations." NAACP v. Alabama ex rel Patterson, 357 U.S. 449, 462 (1958); *see* Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 558 (1963) (rejecting attempt of state legislative committee to require NAACP to produce membership records); Shelton v. Tucker, 364 U.S. 479, 490 (1960) (striking down state statute requiring that teachers list all of their association memberships in the previous five years.)

[1] New Jersey also recognizes "bodily privacy," concerning the protection of people's physical selves against governmental intrusion. *See, e.g.*, In re Quinlan, 70 N.J. 10 (1976) ("right to die"); State v. Saunders, 75 N.J. 200 (1977) (consensual sexual relations between adults); In re Grady, 85 N.J. 235 (1981) (sterilization); Right to Choose v. Byrne, 91 N.J. 287 (1982) (procreation); Greenberg v. Kimmelman, 99 N.J. 552 (1985) (right to marry).

That Shirley Reid's use of her computer occurred in her home also has constitutional significance. The privacy of the home is fundamental, woven into the very fabric of life in New Jersey. Doe v. Poritz, 142 N.J. at 87 (privacy interest in home address information); *see also* Berger v. New York, 388 U.S. 41, 50 (1967) (wiretap of a home phone constitutes a search). Thus, this case involves "*territorial privacy*," which limits intrusion into domestic and other environments such as the home, the workplace, or public space. *See, e.g.*, State v. Baker, 81 N.J. 99, 109 (1979) (family composition). Indeed, essential to the balance between state power and individual liberty is "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion." Kyllo v. United States, 533 U.S. 27, 31 (2001) (thermal imaging). The aphorism that "a man's house is his castle" dates from at least 1604, and the courts have consistently registered concern when the doors of citizens' homes are "broken open" by the government. *See* Wilson v. Layne, 526 U.S. 603, 610 (1999) (media ride-along violates privacy of the home). Like the ability to engage in phone calls confidentially from one's home, so too is the right to make confidential electronic communications for one's home computer deserving of protection.

A. The Private Information ISP Providers Compile Is Vast and Includes Sensitive Personal Information.

By necessity, in order to use the Internet, New Jersey citizens must communicate through ISPs. ISPs are conduits, not parties to the communication. Though they screen communications for viruses, etc., this screening is performed not by humans, but by software. *See* Warshak, *supra*, U.S. App. Lexis 14297 at *42-43.

An IP or "Internet Protocol" address is a number that uniquely identifies a computer or other Internet[2] device,

[2] A brief discussion of the Internet's basic workings may be of aid to the Court. For an introductory volume on the subject suitable for a lay audience, see Preston Gralla, How the Internet Works (MacMillan Computer Publishing 1999): The Internet is a global network of many individual computer networks, all speaking the same networking protocol, the **Internet Protocol** (**IP**). Every computer connected to the Internet has an **IP address**, a unique numeric identifier that can be "static", i.e. unchanging, or may be "dynamically" assigned by your ISP, such that your computer's address changes with each new Internet session. More sophisticated networking protocols may be "layered" on top of the IP protocol, enabling different types of Internet communications. For instance, **World Wide Web (Web)** communications are transmitted via the HypterText Transfer Protocol (**HTTP**) and **e-mails** via the Simple Mail Transport Protocol (**SMTP**). Additional protocols use their own types of addresses. For example, to download a **Web page** you need its **Web address**, known as a Uniform Resource Locator (**URL**) (e.g., <www.eff.org>. To exchange e-mails both the sender and recipient need e-mail addresses (e.g., user@isp.com). Computers that offer files for download over the Internet are called **servers** or **hosts**. For example, a computer that offers Web pages for download is called an HTTP server or Web host. The amount of data in an Internet communication is measured in computer bytes. Communications to and from an Internet-connected computer occur through

similar to the way a telephone number identifies a telephone. *See* Klimas v. Comcast, 465 F.3d 271, 273 (6th Cir. 2006)("Any computer from which a person accesses the internet is assigned an IP address, which may be either 'static' (remain constant) or 'dynamic' (change periodically)."). Just as one cannot use the telephone system without a telephone number assigned by your telephone company, one cannot use the Internet without an IP address (e.g., 111.222.255.4) assigned by one's ISP.[3]

Unlike most phone numbers, however, there are no publicly available directories of IP addresses or email addresses. Thus, an IP address or email address can only be linked to an individual's true identity by her ISP. In this case, for example, a member of the public could not

---

65,536 different computer software **ports**. Many networking protocols have been assigned to particular port numbers by the Internet Engineering Task Force. For example, HTTP (Web) is assigned to port 80 and SMTP (e-mail) is assigned to port 25.

[3] Blocks of IP addresses are delegated to ISPs. As part of providing Internet service, the ISP then delegates one or more IP addresses to its subscribers, and can maintain records of which IP addresses are assigned to each subscriber. By proxy, these records turn IP addresses into information that can uniquely identify ISP subscribers. If the subscriber is a small enough group (as with a family at home), an IP address is as useful in identifying a person as a home telephone number. The only exception is when one uses another's Internet connection, such as at work, a public library, a school, or a private home network.

obtain defendant's name merely from knowing her IP address; only Comcast holds that information.

Another important difference between IP addresses and phone numbers is that an IP address can reveal substantially more about an individual than, for example, the phone numbers she dials. Even "basic subscriber information,"[4] has significant constitutional value.

When an individual accesses a website or sends an email, her IP address is typically logged on the computer system with which she is communicating. "When a URL, or website name, is typed into internet-browser software, a network of computers is able to connect to a corresponding IP address, permitting the transmission by internet of various types of information between the two addresses. [ISPs] have the capacity to maintain databases containing a history of the linkages created by such transmissions." 465 F.3d at 273.

[4] "Basic subscriber information" comprises name; address; telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; local and long distance telephone connection records or records of session times and durations; length of service, including start date, and types of services utilized; and means and source of payment for such service, including any credit card or bank account number. *See* N.J.S.A. 2A:156A-29f.

The ISP can record of all the sites a person visits and all the emails she sends. The ability to link an IP address or email address to a person therefore involves enormous privacy ramifications.

As internet privacy expert Professor Daniel Solove writes:

> On the surface, a list of IP addresses is simply a list of numbers; but it is actually much more. With a complete listing of IP addresses, the government can learn quite a lot about a person because it can trace how that person surfs the Internet. The government can learn the names of stores at which a person shops, the political organizations a person finds interesting, a person's sexual fetishes and fantasies, her health concerns, and so on.

Daniel Solove, *Reconstructing Electronic Surveillance Law*, 72 Geo. Wash. L. Rev. 1264, 1287 (2004).

The problem is not merely hypothetical. According to its website, www.comcast.com/customerprivacy, Comcast currently collects and stores information about its high-speed Internet users when they:

> send and receive e-mail, video mail, and instant messages; transfer and share files; make files accessible; visit websites; place or receive calls; leave and receive voice mail messages; use the Comcast Digital Voice Center (where available); establish custom settings or preferences; communicate with [Comcast] for support; or otherwise use the services and their features.

Through this broad array of activities, Comcast collects:

- billing, payment, and deposit history;

- additional service information;
-customer correspondence and communications records;
- maintenance and complaint information;
- records indicating the number of television sets, set-top boxes, modems, or telephones connected to [Comcast's] cable system; and
- additional information about the service options [users] have chosen

Id. This is an enormous amount of personal information, that, taken as a whole, could provide a "virtual current biography" of the user. McAllister, 184 N.J. at 31. Failing to recognize the privacy interests in this personal information would significantly erode the privacy protections that New Jersey has long recognized.

Doe v. Poritz directly references the type of linking that occurred in Shirley Reid's case. "We believe a privacy interest is implicated when the government assembles those diverse pieces of information into a single package and disseminates that package to the public, thereby ensuring that a person cannot assume anonymity..." 142 N.J. at 87. The Court found that the state's interest in the disclosure of a sex offender's information outweighed the invasion of privacy. Id. at 88-89. In the case of an IP address and contact information, no such overwhelming countervailing public interest exists.

Furthermore, no public disclosure occurs that might reduce the legitimacy of a privacy interest in one's IP

address. The public generally cannot link an IP address to a name, home address, phone number, email address, or any of the information provided by Comcast to the police, although some of that information may be available, separately, to the public. "An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form." Id. at 83. Although Shirley Reid's IP address may be captured publicly, and her contact information may be in the phone book, these facts by themselves should not be permitted to destroy her privacy online.

There is a fundamental flaw behind failing to protect the privacy of subscriber information, or "envelope information." As Professor Solove describes, "The difficulty is that the distinction between content and envelope information does not correlate well to the distinction between sensitive and innocuous information. Envelope information can be quite sensitive; content information can be quite innocuous." Reconstructing Electronic Surveillance Law, *supra*, 72 Geo.Wash.L.Rev. at 1288. Professor Orin Kerr acknowledges that "Solove is correct that in particular circumstances and subject to particular assumptions, noncontent information can

sometimes yield the equivalent of content information," although he dismisses this on grounds that it is a rare scenario. Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it, 72 Geo.Wash.L.Rev. 1208, 1243 n.142 (2004). But the law does not and should not dismiss privacy concerns merely because an invasion is uncommon.

New Jersey cases involving other kinds of third-party subpoenas provide further support along these lines. In McAllister, *supra*, this Court held that "under the New Jersey Constitution, citizens have a reasonable expectation of privacy in bank records." 184 N.J. at 19.

> To be sure, bank customers voluntarily provide their information to banks, but they do so with the understanding that it will remain confidential. A bank customer may not care that employees of the bank know a lot about his financial affairs, but it does not follow that he is indifferent to having those affairs broadcast to the world or disclosed to the government.

Id. at 31 (internal citation omitted).

In McAllister, *citing* Burrows v. Superior Court, 13 Cal.3d 238, 247 (1975), this Court emphasized that technological advances "have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds." 184 N.J. at 31. Particularly virulent risks emerge when

personal information is compiled by one entity. As this Court recognized in McAllister, bank records individually may be "a veritable chronicle of the mundane," but "when compiled and indexed, individually trivial transactions take on a far greater significance." Id. at 30. Here, as in McAllister, law enforcement must not be able to obtain large amounts of personal information about citizens without proper justification.

B. The Right to Anonymous Speech, Protected by the First Amendment, Is Undermined By Disclosure of ISP Information.

At the intersection of privacy and free speech is anonymity. Anonymity is an essential device to protect individuals against governmental overreaching, from whistleblowers to pamphleteers. Anonymity "exemplifies the purpose behind the Bill of Rights, and the First Amendment in particular: to protect unpopular individuals from retaliation - and their ideas from suppression - at the hand of an intolerant society." McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

Always a source of discomfort to law enforcement, anonymity is an important component of democratic participation, because it can be essential for forthright expression. "Identification and fear of reprisal might deter perfectly peaceful discussions of public matters of

importance." Talley v. California, 362 U.S. 60, 65 (1960). The U.S. Supreme Court has held that protecting anonymity is necessary to foster speech about unpopular views. "Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all." Id. at 64.

The First Amendment therefore guarantees the right to speak anonymously. McIntyre, 514 U.S. at 347, 357. Interestingly, Justice Clarence Thomas's concurring opinion discusses the role of anonymous political speech in New Jersey in particular. Id. at 362 (Thomas, J., concurring).

The U.S. Supreme Court has also stated that First Amendment protections apply to speech on the Internet. Reno v. ACLU, 521 U.S. 844, 885 (1997). The fact that speech has been transmitted over the Internet, through an ISP, does not strip the speech of its constitutional protection.

This Court has stated that state constitutional protection of free speech is "the most substantial in our Constitutional scheme." New Jersey Coalition Against War in the Middle East v. JMB Realty, 138 N.J. 326, 363 (1994). To protect the free speech right of computer users in New Jersey, this Court must acknowledge the chilling effect of use of third-party subpoenas by law enforcement to obtain information about computer communications.

Governmental surveillance, including surveillance in cyberspace, can deter speakers from stating their views. This chilling effect carries a significant risk of harm to democratic values. The secret ballot box, for example, was conceived to protect voters because anonymity, rather than visibility, makes political dissention safer. "Bronco" a.k.a. C.R. Scott, "Benefits and Drawbacks of Anonymous Online Communication: Legal Challenges and Communicative Recommendations." In S. Drucker (Ed.), 41 Free Speech Yearbook 127, 132 (2004). Similarly, requiring political canvassers to wear badges violates the First Amendment protection of anonymity. Buckley v. American Const. Law Found, 525 U.S. 182, 197 (1999).

From the anonymous publication of the Federalist Papers to anonymous sources such as "Deep Throat" during the Watergate scandal, anonymity has played and continues to play an important role in American democracy. Anonymous communication on the Internet plays a similar role. Online anonymity must be protected because it is used for purposes that reflect democratic values: (a) facilitating the flow of communication on public issues without killing the messenger (e.g., tiplines, whistleblowing, unsigned political communication); (b) obtaining sensitive information (e.g., for research); (c) focusing attention on

message content rather than status of source; (d) encouraging reporting, sharing, etc. for stigmatized situations; (e) protecting one from subsequent contact (e.g., anonymous donors); (f) avoiding persecution and retaliation for one's beliefs; (g) encouraging risk-taking, innovation and experimentation; and (h) enhancing play/recreational interaction.

Other reasons for anonymous speech include:

> having less relational status than the message receiver, needing to convey sensitive or suspect information, having low concerns about credibility and low need for credit…. Users may desire online anonymity in situations where they have been harassed/stalked, experienced previous embarrassment, wish to avoid recognition by others on multiple lists, want to voice controversial statements, or need to discuss personal/intimate topics. In all these instances, individuals are able to speak more freely (or even do so at all) because of the anonymity provided.

"Bronco," supra, 41 Free Speech Yearbook at 127.

These long-standing rights to anonymity and privacy are critically important to a modern medium of expression, the Internet. As the U.S. Supreme Court recognized, the Internet offers a new and powerful democratic forum in which anyone can become a "pamphleteer" or "a town crier with a voice that resonates farther than it could from any soapbox." Reno v. ACLU, 521 U.S. at 870. Expansion of the

Internet has created countless new opportunities for discourse and self-expression, ranging from the private diary to the multi-million-reader broadcast. The medium hosts tens of millions of dialogues carried out via e-mail publications, Web publications, Usenet Newsgroup message boards, and more, as individuals and associations use the Internet to convey their opinions and ideas whenever they want and to whomever cares to read them.

Many of these millions of dialogues occur anonymously or pseudonymously. Most e-mail providers, including free Web-based services such as Yahoo! Mail and Hotmail, allow subscribers to create e-mail accounts using pseudonyms or pseudonymous e-mail addresses, such that subscribers can send messages or subscribe to newsletters without disclosing their names. Subscribers who post to newsgroups hosted on Usenet servers, as well as other message board services, such as Yahoo! Groups, are identified only by e-mail address, which again may be pseudonymous. Similarly, hosts of online diaries and journals, known as "weblogs" or "blogs," allow subscribers to publish anonymously, while readers may post anonymous comments. Anonymity and pseudonymity are widespread on

the Internet, and crucial to its value as an expressive medium.

For these reasons, basic subscriber information, including anonymous IP addresses, implicate constitutional liberties that must be protected by this Court.

C. New Jersey Case Law and Statutes Have Recognized the Significance of ISP Information.

1. State v. Evers Supports the Proposition that ISP Information Falls Under the Privacy Protections of the New Jersey Constitution.

In a decision that would seem appropriate under New Jersey search and seizure jurisprudence, the Sixth Circuit recently decided in Warshak v. U.S., -- F.3d --, 2007 U.S.App. Lexis 14297 (6th Cir. 2007), that people have a reasonable expectation of privacy in disclosures made to ISP where no human reviews the information transmitted across the ISP's portals. The same conclusion flows from this Court's decision in State v. Evers, 175 N.J. 355 (2003).

This Court's decision in Evers, specifically address the obtaining of ISP information. While decided against the defendant, the case actually provides support for suppressing the ISP information obtained in the present case. The Court accepted "that defendant has a privacy interest sufficient to invoke standing to challenge the

constitutionality of the use of the subscriber information to procure a New Jersey warrant." Id. at 370 (internal citations omitted). It was only because the persons who obtained the information were not New Jersey government actors that this Court did not suppress the information. The Court wrote:

> No purpose would be served by applying New Jersey's constitutional standards to people and places over which the sovereign power of the state has no power or control. *See State v. Mollica*, 114 *N.J.* 329, 347, 554 *A.*2d 1315 (1989) (holding "protections afforded by the constitution of a sovereign entity control the actions only of the agents of that sovereign entity"). Article I, Paragraph 7 of our State Constitution protects the rights of people within New Jersey from unreasonable searches and seizures by state officials, and its jurisdictional power extends to agents of the state who act beyond the state's borders in procuring evidence for criminal prosecutions in our courts. Our State Constitution has no ability to influence the behavior of a California law enforcement officer who does not even know that New Jersey has an interest in a matter he is investigating.

Id. The Court thus implied that a more stringent analysis would have been required if New Jersey officials engaged in the act of obtaining ISP information in which a "defendant has a privacy interest" -- as is the case currently before the Court. Id.

2. The New Jersey Legislature Recognized the Importance of Confidentiality of ISP Information When It Addressed Third Party

Subpoenas for Investigations of Library Records.

A useful example of the nexus between privacy interests, First Amendment rights, and third-party subpoenas arises in the context of law enforcement investigations of libraries. Surprisingly often, libraries receive third-party subpoenas from law enforcement officers. In Hasbrouck Heights, New Jersey, for example, police excoriated a librarian who asked for a subpoena before releasing the name of a library patron. *See* "Library Chief Draws Cops' Ire," *Bergen Record* June 22, 2006. Local authorities in Ringwood asked a public library to monitor all computer users after someone used a public library computer to hack a website. *Bergen Record* July 5, 2001. Four librarians in Connecticut received National Security Letters and remained under a gag order until the USA Patriot Act was reauthorized in 2006. *New York Times*, April 13, 2006.

Libraries are a species of ISP because they provide Internet services to people who do not have computers at home. *See, e.g.*, 47 U.S.C. §230(f)(2)(libraries recognized as ISPs). *See also* Zeran v. America Online, 129 F.3d 327, 330 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998). (This immunity provision of the Communications Decency Act

was not challenged in Reno v. ACLU, 521 U.S. 844 (1997); it remains in full force and effect.)

By virtue of their mission to connect people with ideas, libraries embody First Amendment principles. Kreimer v. Morristown, 958 F.3d 1242 (3d Cir. 1992) (First Amendment right to use library materials).

The New Jersey Legislature specifically invested librarians with an obligation to challenge third-party subpoenas, for the purpose of vindicating the free speech rights associated with anonymity. The use of third-party subpoenas is specifically restricted by statute.

The library confidentiality statute, N.J.S.A. 18A:73-43.1 to 18A:73-43.3, protects the right to read anonymously. In pertinent part, the statute provides:

> Library records which contain the names or other personally identifying details regarding the users of libraries are confidential and shall not be disclosed except in the following circumstances:
>
> a. The records are necessary for the proper operation of the library;
> b. Disclosure is requested by the user; or
> c. Disclosure is required pursuant to a *subpoena issued by a court* or court order.

N.J.S.A. 18A:73-43.2 (emphasis added).

Under this law, libraries may not disclose records that contain names, addresses or other personally identifiable information about library customers. A library

record is defined under the statute as "any document ... the primary purpose of which is to provide for control of the circulation or other public use of library materials." N.J.S.A. 18A:73-43.1. This means that if the police want access to computers to check patrons' e-mail, review borrowing records, or track websites, the police must first get a "subpoena issued by a court" or court order.

The requirement that a subpoena be "issued by a court" explicitly requires a measure of judicial supervision of third-party subpoenas directed to libraries. This explicit statutory protection of anonymity in the library emphasizes the Legislature's determination to ensure that the people of New Jersey can count on valid subpoena process and a measure of judicial oversight to limit governmental investigations.

Ultimately, this is for the purpose of preserving the Internet as a robust medium of communication.

> The free exchange of ideas on the Internet is driven in large part by the ability of Internet users to communicate anonymously. If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discover, this would have a significant chilling effect on Internet communication and thus on basic First Amendment rights.

Doe v. 2TheMart.com, 140 F.Supp.2d 1088, 1093 (W.D. Wa. 2001). Discovery requests seeking to identify anonymous Internet users should be subject to judicial oversight.

III. THIRD-PARTY SUBPOENAS THAT IMPINGE UPON CONSTITUTIONAL INTERESTS MERIT JUDICIAL SCRUTINY

Abuse of the subpoena power is a grave concern. Properly limited, a subpoena does not constitute an unreasonable search or seizure, even when it compels production of evidence in which there is a privacy interest. *See, e.g.*, In re Addonizio, 53 N.J. 107, 118 (1968).

But the potential for abuse is acute when subpoenas are issued to third parties, such as ISPs. In principle, a subpoena can be challenged prior to the seizure of documents and things. R. 1:9-1. But third parties need not notify the target, and may have no incentive to challenge subpoenas by mounting motions to quash, even if the subpoenas are defective.

When non-governmental parties attempt to obtain identifying information from ISPs, courts have held that subpoenas for this information must meet heightened standards, such as providing notice to the target of the subpoena. *See, e.g.*, Dendrite Int'l, Inc. v. John Doe No. 3, 342 N.J. Super. 134 (App. Div. 2001). In criminal cases,

the stakes are much higher. Piercing a speaker's anonymity, surreptitiously, by the police, with jail time as a possible consequence, demands a more critical assessment of the government's position.

This Court must require at least minimum standards for the government when it uses third party subpoenas and, where constitutional rights are at stake, a measure of judicial oversight. McAllister, 184 N.J. at 33. When the government issues subpoenas that compel third parties to reveal the identities of anonymous speakers, the government should meet standards at least as exacting as the standards required of non-governmental actors.

A. Judicial Oversight Is Required Where Constitutional Rights Are At Stake.

Where third-party subpoenas compromise privacy interests secured by the state constitution, or impact the rights guaranteed by the First Amendment, the courts must scrutinize the subpoenas and hold the State to its promise to protect these constitutional rights.

Service providers like Comcast control users' access to the web, where great amounts of personal information may be contained. "If we fail to afford protection against governmental snooping in these files, our right of privacy will evaporate. Moreover, if we fail to protect the records

of third-party providers, there will be a tremendous disincentive created against using these services." Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 72 Geo. Wash. L. Rev. 1557, 1598 (2004).

In Dendrite Int'l, Inc. v. John Doe No. 3, 342 N.J. Super. 134 (App. Div. 2001), the Appellate Division established a framework for trial courts to use when considering whether an ISP should be compelled to disclose the identities of online speakers. The court recognized that lawsuits could easily be brought for the primary purpose of discovering the identities of individuals who were critical of a plaintiff, and not for the meritorious purpose of seeking legal redress.

Dendrite set forth a four-part standard: First, a trial court must require the plaintiff to undertake efforts to notify the anonymous posters that they are the subject of a subpoena. Second, the plaintiff "must identify and set forth the exact statements … the plaintiff alleges constitutes actionable speech." Third, the pleadings must establish a *prima facie* cause of action, and, fourth, the court must balance the defendant's First Amendment rights

of free speech against the strength of the *prima facie* case. Id. at 141.

Similarly, Doe v. 2TheMart.com, 140 F.Supp.2d 1088 (W.D.Wash. 2001), held that a subpoena for the identities of anonymous speakers required heightened standards to protect the right to speak anonymously. The court cited four factors to determine whether a subpoena can be issued:

> the subpoena seeking the information [must be] issued 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 disprove that claim or defense is unavailable from any other sources.

Id. at 1089-93. Other courts have articulated similar tests. *See, e.g.*, Columbia Ins.Co. v. Seescandy.com, 185 F.R.D. 573 (N.D.Cal. 1999). *See also* Immunomedics v. Doe, 342 N.J. Super. 160 (App. Div. 2001) (affirming trial court's denial of an anonymous poster's motion to quash a subpoena).

In civil cases like Dendrite, a plaintiff who obtains the identity of an anonymous speaker can subject the speaker to embarrassment, harassment and ridicule. For this reason, the Appellate Division adopted safeguards to prevent the chilling effect that unmeritorious suits would have on the freedom of speech. 342 N.J. Super. at 151. "The

guiding principle," the Appellate Division stated, "is a result based on a meaningful analysis and a proper balancing of the equities and rights at issue." Id. at 142.

The same principle must attach where criminal investigations touch rights that are constitutionally protected. Indeed, citizens are subject to even greater consequence (namely, potentially criminal consequences and a chill upon free speech) when it is the government seeking their information, and third-party entities like ISPs do not have the incentive to challenge the governmental request that the target of the request does.[5]

The criminal law implications are obvious. Simply put, in criminal cases, the stakes are much higher. Piercing a speaker's anonymity, surreptitiously, by the police, with jail time as a consequence, demands a more critical balancing of rights. See, e.g., State v. Hempele, 120 N.J. 182, 205 (1999) ("Although a person may realize

[5] It cannot avail the State to invoke the rationale for *ex parte* warrant; such a rationale does not apply with respect to third-party subpoenas. For warrants, an *ex parte* procedure and the invasive search and seizure that follow are justified because of the exigencies of law enforcement and the practical reality that a suspect, if notified ahead of time, has a motive to destroy evidence or otherwise frustrate the search for particularly incriminating records. These exigencies do not attach to subpoenas, which must provide advance notice to allow for judicial intervention when motions are made to quash.

that an unwelcome scavenger might sort through his or her garbage, 'such expectations would not necessarily include a detailed, systematized inspection of the garbage by law enforcement personnel'"). Before piercing the anonymity of online computer users, the government must therefore, at the very least, elicit appropriate judicial oversight or give notice to the target of the investigation.

This Court's decision in McAllister addressed the due process problems with relying merely on third-party subpoenas, without notice or judicial oversight. This Court explained that, generally, the issuance of a grand jury subpoena *duces tecum* based on a relevancy standard satisfies the constitutional prohibition against improper government intrusion. McAllister, 184 N.J. at 36. However, as further noted by this Court:

> A problem arises, however, when the prosecutor executes a grand jury subpoena duces tecum on a third party, such as a bank. Although the bank can oppose the subpoena on the same procedural grounds as any other party under subpoena, the bank does not have available the arsenal of substantive arguments that the investigation's target could advance. Furthermore, as a practical matter, the bank simply does not have the same incentive to vigorously assert even its limited defenses against the State's request.

McAllister, 184 N.J. at 38.

Where third-party subpoenas compromise privacy interests secured by the state constitution, or impact the

rights guaranteed by the First Amendment, the courts must exercise judicial oversight so as to ensure the necessary protections and process.

Colorado Supreme Court applied this principle to an executable search warrant in Tattered Cover v. City of Thornton, 44 P.3d 1044 (2002). Police investigating a methamphetamine lab subpoenaed a bookstore to find out who had purchased a how-to book for manufacturing methamphetamine. Under the state constitution, the Colorado Supreme Court held that the bookseller was entitled to challenge the search warrant in an adversarial hearing, prior to the execution of the warrant.

The Tattered Cover case is particularly interesting because the court acknowledged that, otherwise, the police could have executed the subpoena before giving a court the opportunity to consider the constitutionality of the warrant. It cited the "grave concern" that a "chilling effect felt by the general public" would result from the very fact of governmental discovery of book-buying purchases. Id. at 1060.

Ultimately, the needs of law enforcement are not determinative; they must be balanced against the rights of the targets and the third parties. Here, the rights at issue touch upon the very right to speak anonymously.

B. When Government Acts Pursuant to Police Powers, the Judiciary Must Protect Against Prosecutorial Overreaching, as Part of the Democratic System of Checks and Balances

This Court must exercise its institutional authority to ensure that Constitutional interests are preserved as new communications techniques emerge. The digital revolution has given modern law enforcement unprecedented power to conduct surveillance, surreptitiously obtain personal information, exercise unlimited discretion, monitor disfavored individuals, and engage in discriminatory profiling. These practices typically do not result from malicious intent or a desire for domination.

Justice Brandeis was prescient in his dissent in Olmstead v. United States, 277 U.S. 438 (1928). Not only did he predict that "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." Id. at 474 (Brandeis, J., dissenting). He recognized the allure of technology to effect social control: "Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. … The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning

but without understanding." Id. at 478 (Brandeis, J., dissenting).

This Court is invested with the unique institutional competence to apply constitutional principles to police practices in New Jersey. As such, it is the protector of the trust of the people of this state to guard them against overreaching by law enforcement officers.

Trust enhances both the legitimacy of the democratic state and the ability of the government to carry out its responsibilities. Technological change is, or should be, accompanied by the expectation that the state will exercise a duty of care. This duty of care includes holding police practices to restraints that attached prior to the digital revolution, restraints that embody the principles of due process and limited government.

Law enforcement officials cannot, working alone, strike the balance between order and liberty. They experience tremendous pressure to capture criminals, solve notorious crimes, maintain control, and prevent acts of violence and terrorism. Absence of restraint is bound to characterize unchecked police power. *See e.g.*, State v. Soto, 324 N.J.Super. 66 (Law Div. 1996) (racial profiling); State v. Ballard, 331 N.J.Super. 529 (App. Div. 2000) (same). Accordingly, some measure of restraint must be

imposed by the Judiciary as a coordinate branch of government.

One of the most crucial devices for limiting government power is the system of checks and balances. Writing about the separation of powers in *Federalist No. 51*, Madison observed:

> If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: You must first enable the government to control the governed; and in the next place, oblige it to control itself. A dependence on the people is no doubt the primary control on the government, but experience has taught mankind the necessity of auxiliary precautions.

Madison was acutely aware that the "parchment barriers" of the Constitution would fail to check government encroachments of power, and he explained how both the legislative and executive branches could overstep their bounds. *Federalist No. 48*.

Enveloped as they are in tremendous responsibilities, law enforcement officials cannot reasonably be expected to maintain an unbiased and balanced perspective. Just as the colonists despised writs of assistance because they authorized sweeping searches and seizures without any evidentiary basis, modern Internet users should not be

expected to tolerate unchecked police surveillance of their computer use.

Trust has a rational basis. In government, it can thrive only when state actors perform their roles satisfactorily. Trust, in the police and in this Court, is vulnerable if these institutions discard or discount the minimum requirements for issuing a valid subpoena to investigate the likes of Shirley Reid.

IV. THE DOUBLY DEFECTIVE SUBPOENA FOR INFORMATION ABOUT REID VIOLATED STATE STATUTES

The fact that the State used a municipal subpoena in violation of state statutes is not in dispute, State v. Reid, 389 N.J. Super. 563, 568 (App. Div. 2007); the question is whether the State may use the unlawfully acquired information.

The State's acquisition of defendant's information was doubly defective. A proper subpoena may only be used to obtain basic subscriber information, per N.J.S.A. 2A:156A-29f. Here, by contrast, the State demanded records of all activity associated with the IP address for a three-hour period,[6] information it was not empowered to obtain under section 29f.

[6] The State sought "[a]ny and all information pertaining to [Ms. Reid's] IP address, which occurred on 08-24-04 between

The records it sought could not have been obtained by the State without at least a court order. N.J.S.A. 2A:156A-29c; id. at 29e (providing that such orders "shall issue only if the law enforcement agency offers specific and articulable facts showing that there are reasonable grounds to believe that the record or other information[7] pertaining to a subscriber or customer . . . is relevant and material to an ongoing criminal investigation."). Thus, not only did the State use an unauthorized subpoena, no subpoena could obtain the information it demanded, a three-hour window into the defendant's online life. As explained above, the data Comcast disclosed, while less than the State sought,

---

8:00 a.m. and 11:00 a.m. EST." State v. Reid, 389 N.J. Super. 563, 567 (App. Div. 2007).

[7] This "other information" could have included: E-mail "headers" that contain addressing and routing information generated by the e-mail program, including the e-mail address of the sender and recipient(s), as well as information about when each email was sent or received and what computers they passed through while traveling over the Internet; the Web address of every Web page or site accessed; the IP address assigned to the subscriber by the ECSP, and the IP addresses of other Internet-connected computers that the subscriber sends to or receives from; the port number used, indicating the type of networking protocol used (e.g., HTTP, SMTP) and hence the type of communication (e.g., Web page, e-mail); web server logs showing the source (i.e., IP address) of requests to view a particular Web page; connection logs showing when the subscriber connects and disconnects to the Internet; time stamps showing the date and time when each communication is sent or received; the size in bytes of each communication.

exposed information about the Defendant that touched upon privacy interests protected by the state constitution and upon her First Amendment rights.

Without a remedy for such statutory violations, the State will have no incentive not to overreach, in hope of obtaining more data than it is entitled to. In this case, suppression is clearly warranted.

CONCLUSION

For all the reasons set forth above, this Court must recognize a constitutionally-protected privacy interest and limit the State's use of third-party subpoenas to pierce the anonymity of New Jersey residents who access the Internet.

_____

Grayson Barber
GRAYSON BARBER, L.L.C.
Counsel for *Amici Curiae*

American Civil Liberties Union of New Jersey Foundation

Electronic Frontier Foundation

Electronic Privacy Information Center

Freedom to Read Foundation

Privacy Rights Clearinghouse

New Jersey Library Association

Dated: July 5, 2007