STATEMENT ON THE CONSTITUTIONALITY OF THE DISCLOSURE OF NAME AND ADDRESS INFORMATION FROM PUBLIC RECORDS

Before the New Jersey Privacy Study Commission

By Fred H. Cate
Distinguished Professor
Indiana University School of Law-Bloomington

Newark, NJ, November 12, 2003

Mr. Chairman and Members of the Commission:

My name is Fred Cate and I am a Distinguished Professor at the Indiana University School of Law—Bloomington. For 13 years I have researched and taught about information privacy issues. I am the author of three books and dozens of articles in this field. I have testified many times before Congress and state legislatures and consulted with a number of government agencies, not-for-profit groups, and businesses about privacy matters. I currently advise the Department of Defense Technology and Privacy Advisory Committee.

The tension between privacy and access to public records was one of the first subjects that I addressed in my privacy work. In 1999 I co-authored with Richard Varn, CIO of the State of Iowa, a report on *The Public Record: Information Privacy and Access—A New Framework for Finding the Balance.* My research in this area and my appearance here today have been supported by the Coalition for Sensible Public Records Access, a not-for-profit group funded by businesses that aggregate and enhance public records for public use. I do not speak for or represent CSPRA or any of its members. I am testifying on my own behalf as a scholar of privacy and First Amendment law.

I am grateful for the opportunity to testify. I applaud the wisdom of the State of New Jersey in creating this Commission and your commitment to addressing these critical issues. Other states and students of privacy law are likely to look to your findings. This is why I believe it is so important to correct a misimpression created by the draft report of your Special Directive Subcommittee concerning the legal privacy interest in name and address information found in public records.

The September 8, 2003, draft report posted on the Commission's website concludes that "the Special Directive Subcommittee believes the United States Constitution explicitly protects the home as a refuge from governmental action, and that this protection extends to the disclosure of home addresses and home telephone numbers."[1] Under the heading "Constitutional Support," the report asserts that "[t]he New Jersey Supreme Court and the United States Court of Appeals for the Third Circuit (the federal court that governs New Jersey) have held that citizens have a constitutional right to privacy in their home address."[2] "Therefore," the Subcommittee writes, "disclosure of home addresses under OPRA may violate a constitutionally protected right to privacy."[3]

I believe these assertions are incorrect as a matter of law. They are largely unsupported by the cases cited in the report. More importantly, they contradict clear holdings of other federal courts that are not included in the Subcommittee's report. This is not a question of quibbling over a fine point of constitutional theory. The report repeatedly makes unfounded assertions about the scope of the

constitutional right of privacy. Because the Constitution acts as an absolute prohibition on governmental acts that are inconsistent with it, if left uncorrected, these assertions threaten to mislead the Commission in its recommendations about the extent to which address and telephone information in public records may be made public, as well as others who will look to the Commission's findings.

I therefore wish briefly to discuss the Subcommittee's claims and to identify some of the omitted evidence contradicting them.

THE "RIGHT TO PRIVACY"

Scholars and courts have identified many rights to privacy in the Constitution. The Supreme Court alone has used the term to describe an individual's constitutional right to be free from unreasonable searches and seizures by the government;[4] the right to make decisions about contraception,[5] abortion,[6] and other "fundamental" issues such as marriage, procreation, child rearing, and education;[7] the right not to disclose certain information to the government;[8] the right to associate free from government intrusion;[9] and the right to enjoy one's own home free from intrusion by the government,[10] sexually explicit mail[11] or radio broadcasts,[12] or other intrusions.[13]

These are important rights and the Subcommittee report cites to many of them, but most—for example, all of the rights relating to making fundamental decisions—have nothing to do with the government's disclosure of address and telephone numbers from public records. In fact, few of those rights involve privacy of information at all. Virtually all of those that do concern the question of whether the government may *collect*—rather than *disclose*—information. The Subcommittee report addresses many cases concerning these rights, most of which are based in the Fourth Amendment's protection against warrantless or unreasonable searches and seizures. But my understanding of the Governor's Special Directive is that it asks whether the government should *disclose* address and telephone number information it has collected, not whether it should *collect* that information in the first place. These are very different questions, and it is important to keep them separate. It comes as a surprise to many, but the Fourth Amendment, which poses such a high burden for the government to collect information, actually says nothing about what the government can or should do with it once collected.

The Subcommittee report's discussion of cases interpreting federal and state open records laws is also irrelevant to the issue of whether there is a constitutional prohibition on disclosing address and telephone information. Again, the difference may seem technical, but it is legally significant. Open records laws—like all statutes, executive orders, and common law—reflect policy decisions that may be altered by the Legislature or the Governor. The Constitution and judicial interpretations of it, by contrast, are commands that bind the other branches of government and trump all other laws. So a statutory right cannot be the basis for a constitutional right.

There is in fact only one U.S. Supreme Court that articulates a *constitutional* right in nondisclosure of information, although it does so in the context of nondisclosure *to* the government, rather than any obligation of nondisclosure *by* the government. In 1977, the Supreme Court decided *Whalen v. Roe*, a case involving a challenge to a New York statute requiring that copies of prescriptions for certain drugs be provided to the state, on the basis that the requirement would infringe patients' privacy rights.[14] The Court wrote that the constitutionally protected "zone of privacy" included "the

individual interest in avoiding disclosure of personal matters . . . .”[15] Nevertheless, having found this new privacy interest in nondisclosure of personal information, the Court did not apply strict scrutiny—which it typically reserves for cases involving “fundamental” interests. Instead, applying a lower level of scrutiny, the Court found that the statute did *not* infringe the individuals’ interest in nondisclosure.[16] In fact, the Supreme Court has never decided a case in which it found that disclosure *to or by* the government violated the constitutional privacy right recognized in *Whalen*.

THE SUBCOMMITTEE’S CASES

With no Supreme Court precedent available to support its conclusion about the existence of a constitutional obligation not to disclose address and telephone information found in public records, the Subcommittee cites to five cases: a New Jersey Supreme Court case (*Doe v. Poritz*[17]) and four Third Circuit Court of Appeals cases (*Paul P. v. Verniero*,[18] *Paul P. v. Farmer*,[19] *A.A. v. New Jersey*,[20] and *United States v. Westinghouse Electric Corp.*[21]). These cases, however, do not support the asserted proposition.

Four of the cases involve challenges to variations of Megan’s Law, which requires public disclosure of information about released convicted sex offenders, including in some instances home address. Despite the fact that all four cases *upheld* the disclosure requirement, as did the U.S. Supreme Court,[22] the Subcommittee nevertheless relies on them because the courts provided dicta that the disclosure of address information “implicates a privacy interest.”[23]

In three of the four cases, the courts explicitly ground the privacy interest they are discussing in statutes—open records laws—not the U.S. or New Jersey Constitutions. Moreover, the courts characterize even the statutory privacy right in very weak terms. The New Jersey Supreme Court, for example, noted that the “interests in privacy may fade when the information is a matter of public record, but they are not non-existent.”[24] The Third Circuit was even more tentative, referring to “[w]hatever privacy interest, *if any*, [that] may exist in the area of one’s residence.”[25] Not surprisingly, given the tenuous nature of this nonconstitutional privacy right, the courts found that it is trumped by the public’s interest—also nonconstitutional in origin—in knowing where convicted sex offenders live. These three cases, therefore, simply do not support the claim that there is a constitutional privacy right in nondisclosure of address and telephone number information from public records.

The fourth Megan’s Law case does involve a challenge based in part on a constitutional right to privacy, but the court merely asserted its existence before describing its weakness and concluding that it was “substantially outweighed” by the public’s interest in access to the information in the sex offender registry.[26]

The final case cited by the Subcommittee involved the application of a statute—the federal Freedom of Information Act—to the disclosure of highly sensitive personal information (i.e., medical records) to the government. Although the court, citing to *Whalen*, found that the interest in

nondisclosure was constitutional, it ultimately concluded that the public interest in requiring disclosure of the information exceeded whatever privacy rights were at stake.[27]

It is unreasonable to analogize, as the Subcommittee does, from these cases to a general constitutional obligation to maintain the secrecy of address and telephone number information. In all of the cases, the disclosures were in connection with sensitive information—either medical records or highly stigmatizing information about sex offense convictions. Whatever privacy interest was at issue either did not concern address information at all or was not in address information alone, but in address information connected with the knowledge that the resident had previously been convicted of a sex offense. These cases thus provide a tenuous basis from which to argue about the privacy interests applicable to run-of-the mill address and telephone information found in property tax records, voting records, and hunting and fishing permit application files. In addition, three of the cases were explicitly discussing statutory—not constitutional—rights. And all five cases *upheld* the disclosure requirement in spite of the privacy interests identified.

Cases holding that the government may require the disclosure of sensitive medical records or information on past sex offense convictions are poor precedent for a claim that the government is constitutionally prohibited from allowing the public access to addresses and telephone numbers contained in public records

PROFESSOR SOLOVE'S RESEARCH

The Subcommittee report refers to the work of Professor Daniel J. Solove, a professor at Seton Hall Law School and a talented young scholar of privacy law. The report refers to testimony of Professor Solove stating that "if New Jersey were to routinely give out home addresses and phone numbers, it would . . . be violating the Constitution (as interpreted by many federal courts of appeal, including, most importantly, the Third Circuit)."[28] Regrettably, I did not hear Professor Solove testify, but it is difficult to believe that this characterization of his statement is accurate.

In his 2002 article, "Access and Aggregation: Public Records, Privacy and the Constitution," Professor Solove offers a similar, but more modest conclusion that the Constitution both "mandate[s] public access to information" and also "obligates the government to refrain from disclosing personal information."[29] Even this conclusion may appear broader than the cases on which it is based would support.

None of the cases to which Professor Solove cites concern the constitutional protection that may attach to address and telephone information in public records. He refers, for example, to *NAACP v. Alabama*,[30] a 1958 case in which the Supreme Court struck down a statute requiring that the NAACP disclose its membership lists. This very important case involved disclosure *to*, not *by*, the government of not merely names and addresses, but of the fact that the information identified people who were members of a political group. Such a requirement, the purpose of which was to undercut support for the NAACP, clearly violated the "freedom to associate" and the "privacy in one's association."[31] The case said nothing about the privacy of routine address and telephone information.

Similarly, Professor Solove cites to *Greidinger v. Davis*,[32] in which the U.S. Court of Appeals

for the Fourth Circuit held that a Virginia law that condition voting on voters providing their Social Security Numbers, which would then be made public, constituted a violation of the fundamental right to vote. The right to vote—not privacy—was the focus of the case, and the information involved was sensitive Social Security Numbers, not address and phone information.

Professor Solove cites to a series of cases involving the right to make fundamental decisions, culminating in *Roe v. Wade*, [33] involving a woman's right to choose to have an abortion. This vital right certainly does not compel the State of New Jersey to withhold name and address information found in public records. Finally, he cites to *Whalen*, for the fact that the Supreme Court has identified, even though it has never upheld, a constitutional interest in individuals not disclosing certain personal information *to* the government.

Collectively, these cases offer little support for the proposition that the Constitution "obligates the government to refrain from disclosing personal information." In fact, Professor Solove's excellent article makes a stronger argument that "even if a state did not have a sunshine law or a common law right of access, the Constitution might be interpreted to require a degree of openness." [34] In any event, it is clear that Professor Solove's article offers scant support for the claim attributed to him in the Subcommittee's draft report that "if New Jersey were to routinely give out home addresses and phone numbers, it would . . . be violating the Constitution."

CONSTITUTIONAL CASE LAW CONTRADICTING THE SUBCOMMITTEE'S CONCLUSION

Federal appellate courts have decided many cases that contradict the Subcommittee's conclusions in its draft report. The clearest example is the 1998 decision by the U.S. Court of Appeals for the Fourth Circuit, striking down the Drivers Privacy Protection Act. [35] The Act required states to restrict access to information contained in motor vehicle records, including the addresses and telephone numbers of vehicle owners and licensed drivers. The court wrote that *"neither the Supreme Court nor this Court has ever found a constitutional right to privacy with respect to the type of information found in motor vehicle records. Indeed, this is the very sort of information to which individuals do not have a reasonable expectation of privacy."* [36]

The court went on to stress that it would be unreasonable to prevent the disclosure of such information because "the same type of information is available from numerous other sources. . . . As a result, an individual does not have a reasonable expectation that the information is confidential. . . ." [37] The court concluded that "such information is commonly provided to private parties. . . . We seriously doubt that an individual has a . . . right to privacy in information routinely shared with strangers." [38]

These conclusions seem remarkably on point: there is no "constitutional right to privacy" with respect to information such as address and telephone numbers; there isn't even a common law "reasonable expectation" of privacy in such information; and there could not be when the information is "routinely shared with strangers." Moreover, although the Supreme Court later upheld the constitutionality of the DPPA on other grounds, having to do with federalism and the Tenth Amendment and not privacy or the First Amendment, it did not see the need to disagree with or in any way distinguish the Fourth Circuit's discussion about the constitutional right to privacy. [39]

The Fourth Circuit's opinion on point is consistent with a wide range of other appellate and Supreme Court opinions on information privacy generally. For example, in 1999 the U.S. Court of Appeals for the Tenth Circuit was presented with a First Amendment challenge to Federal Communications Commission rules that required telephone companies to get opt-in consent from customers before using data about their calling patterns to determine which customers to contact or what offer to make them.[40] The court found that under the First Amendment, the rules were presumptively unconstitutional unless the FCC could prove otherwise by demonstrating that the rules were necessary to prevent a "specific and significant harm" and that the rules were "'no more extensive than necessary to serve [the stated] interests."[41]

The appellate court's words are instructive in the discussion over whether the State should keep name and address information confidential: "the government must show that the dissemination of the information desired to be kept private would inflict *specific and significant harm* on individuals. . . ."[42] To meet that burden, according to the appellate court, requires that the government engage in a "careful calculat[ion of] the costs and benefits associated with the burden on speech imposed by its prohibition." "The availability of less burdensome alternatives to reach the stated goal signals that the fit between the legislature's ends and the means chosen to accomplish those ends may be too imprecise to withstand First Amendment scrutiny."[43]

The court went on to write that:

> Although we may feel uncomfortable knowing that our personal information is circulating in the world, we live in an open society where information may usually pass freely. A general level of discomfort from knowing that people can readily access information about us does not necessarily rise to the level of substantial state interest under *Central Hudson* for it is not based on an identified harm.[44]

It is important to recognize that the Tenth Circuit required that the government articulate a "substantial state interest" even though the court examined the restriction at issue in that case under the less protective *Central Hudson* test applicable to commercial speech. The address and telephone number information at issue before this Commission is found in public records, not commercial advertising, and so is subject to the full protection of the First Amendment.

The logic of the Fourth and Tenth Circuits is consistent with the Supreme Court=s Fourth Amendment jurisprudence. In the face of the Fourth Amendment's explicit constitutional command to protect individuals from government intrusions, the Court has long held that the constitutional protections for privacy only protect *reasonable* expectations of privacy. When evaluating wiretaps and other seizures of private information under the Fourth Amendment, the Supreme Court has long asked whether the data subject in fact expected that the information was private and whether that expectation was reasonable in the light of past experience and widely shared community values.[45] Similarly, virtually all state privacy torts—with the sole exception of commercial appropriation—require that the invasion of privacy be *outrageous* or *unreasonable*.[46] The Supreme Court has struck down laws that did not contain such a requirement.[47]

The Supreme Court reaffirmed the dominance of free expression over privacy interests in the 2001 case of *Bartnicki v. Vopper*.[48] There the Court explicitly balanced the constitutional interests in privacy and expression, and held that the broadcast of even an *illegally intercepted* cellular telephone conversation was protected by the First Amendment: "Exposure of the self to others in varying degrees is a concomitant of life in a civilized community. The risk of this exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press."[49]

SUMMARY

I do not mean to suggest that the Constitution requires New Jersey to provide access to address and telephone information in public records, but rather that it clearly does not prohibit that access and it establishes strong precedent in favor of it. It is up to the Commission to balance the benefits and costs of access, in light of that presumption, to answer the questions posed by the Governor as to whether address and telephone information in public records *should* be accessible to the public.

In certain circumstances—for example, involving undercover police officers and people protected by restraining orders—I believe it is reasonable to conclude that despite the constitutional values served by public access, address and telephone number information should be protected. My research suggests, however, that will not be true in most cases. I thought it might by useful to conclude by briefly summarizing some of the benefits that flow from address and telephone information being generally available from public records.

BENEFITS OF PUBLIC ACCESS TO ADDRESS AND TELEPHONE INFORMATION IN PUBLIC RECORDS

Information to Inform the Public

Access to address information in public records is essential for journalists and other researchers to gather information and inform the public about matters of public importance. In each of the following examples, address and telephone information was critical to identity people, locate them, and match information concerning them:

- *San Francisco Examiner* reporter Candy Cooper discovered that police investigated rapes in upscale Berkeley far more readily than in the crime-infested neighborhoods of Oakland by systematically examining local government records.
- The *St. Petersburg Times* searched public records to discover that a man running for city treasurer had not disclosed that he had filed for personal bankruptcy three times and corporate bankruptcy twice.
- Tampa's News Channel 8 mapped the location of all drug arrests—information obtained from public records—to uncover a narcotics ring across the street from an elementary school.
- The Associated Press matched Mississippi Department of Correction and Department of Education records to discover eight school teachers who had failed to report that they had been convicted of crimes including drug dealing and sex offenses.

In fact, a recent study by Indiana University Knight Journalism Fellow Brooke Barnett found that journalists routinely use public records not merely to check facts or find specific information, but to actually generate the story in the first place. According to that study, 64% of all crime-related stories, 57% of all city or state stories, 56% of all investigative stories, and 47% of all political campaign stories

rely on public records. Access to public record databases is "a *necessity* for journalists to uncover wrongdoing and effectively cover crime, political stories and investigative pieces."[50] Address data is a critical element, not only to find people, but to accurately identify them and match information concerning them.

Information to Verify Identity and Locate Individuals

Public records are a key source of information about citizen addresses. This information is used to locate missing family members, owners of lost or stolen property, organ and tissue donors, and members of associations and religious groups and graduates of schools and colleges; and to identify and locate suspects, witnesses in criminal and civil matters, tax evaders, and parents who are delinquent in child support payments.

The Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75% of the "deadbeat parents" they sought.[51] New York City's Child Support Enforcement Department used public record information supplied by ChoicePoint to recover $36 million over two years from thousand of non-custodial parents.[52]

Law enforcement relies on public record information to prevent, detect, and solve crimes. In 1998 the FBI alone made more than 53,000 inquiries to commercial on−line databases to obtain a wide variety of "public source information." According to then-Director Louis Freeh, "Information from these inquiries assisted in the arrests of 393 fugitives wanted by the FBI, the identification of more than $37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning."[53]

Firestone and Ford Motor Company used public records to identify and obtain current addresses for people who needed to receive information on replacing defective tires.

Information to Update Customer Lists and Improve the Accuracy of Existing Databases

Businesses, not-for-profit groups, and membership organizations face a constant burden and considerable cost to keep their customer and membership lists accurate and up-to-date. Forty-two million Americans move each year and many of them do not think to send their new address to all of the business, alumni groups, charities, political parties, and others with whom they deal.

The cost of losing track of a customer, member, or supporter can be significant. Banks, for example, report spending $200 or more to acquire each customer. Across industries, acquiring a new customer costs on average five times more than keeping one.[54] The risk is not only that organizations lose track of customers or members entirely, but that they end up with several different addresses for the same person without know which is accurate or, in many cases, without even knowing that the multiple records are all for one person. Accurate, up-to-date address information in public records is critical to avoiding the waste, cost, and inconvenience of each business or group updating its address lists on its own.

Public record information also helps businesses and not-for-profit groups accurately and efficiently identify new prospects to receive political, charitable, and religious information based upon

their own interests. As a result, political campaigns, the American Association of Retired People can target its officers only to older Americans, veteran's organizations, and other groups can reach those people most likely to be interested.

Information to Promote Competition and Innovation

Access to address and telephone number information facilitates the creation and growth of new businesses by helping new market entrants, which cannot afford mass market advertising and lack the customer lists of their well-established competitors, to identify and reach potential customers. Basic personal information—including address and telephone data—obtained from public records (such as who owns a house or has a hunting or fishing license, or is licensed to practice a regulated profession) is an especially critical resource for new and smaller businesses—the foundation of economic growth and new jobs. It gives those businesses a cost-effective means to communicate with consumers unfamiliar with their brand name but likely to be interested in their services or products.

For a practical example, consider AOL Time Warner. As a start-up company, AOL mailed free copies of its software to people likely to be interested in Internet access. Prohibiting the fledgling AOL access to information about consumer addresses and computer ownership would have denied consumers information about an opportunity that many of them obviously value, increased the volume of marketing material that AOL would have been required to distribute, and threatened the financial viability of a valuable, innovative service.

Public record data is essential to leveling the playing field for new market entrants. The absence of such information, in the words of Robert E. Litan, Director of the Economic Studies Program and Vice President of The Brookings Institution, and a former Deputy Assistant Attorney General for the United States, would "raise barriers to entry by smaller, and often more innovative, firms and [55] organizations," by making it harder to identify and reach interested potential customers.

Information to Facilitate E-Commerce and Global Competition

The role of public record data is especially critical in e-commerce and national—often global—competition. Today, many businesses never see or physically interact with their customers. Transactions are conducted exclusively over the telephone, Internet or through the mail. Many of today's most successful companies have no physical presence. MBNA, for example, one of the nation's largest credit card issuers, has no physical branches. Few mutual fund providers ever see their investors. Amazon.com exists only in cyberspace. Millions of consumers visit Yahoo and Microsoft and Netscape everyday, but only in virtual space. Dell Computer Corporation sells billions of dollars worth of computers each year solely via the Internet. These and many other new economy companies identify likely customers, market to them, provide them with valuable services and products, and meet their needs solely through information-based relationships.

Public records are a key source of that information and a critical means for verifying other information provided by potential customers. Address information obtained from public records is used to help instantly verify identity when consumers apply for credit or seek to establish new service; determine that the goods ordered are being mailed to the address of the credit card holder who paid for them; detect and correct errors in mailing addresses; and provide current contact information for owners of disused or delinquent accounts.

Information to Prevent Fraud and Identity Theft

Public record information is at the heart of efforts to fight crime, especially identity theft. That information is one of the most effective tools for stemming losses due to bad checks, stolen credit cards,

and other financial frauds. The ability to verify information against that in public records is a key way of ensuring that a customer is who he or she claims to be. Such information is used every day to identify consumers cashing checks, seeking access to accounts, and applying for credit.

Public Support for Responsible Public Records Access

Two of the most recent significant polls addressing public records suggest that the public supports responsible access to public records. The first survey was conducted in September and October 2000 by Opinion Research Corporation, under the direction of Dr. Alan Westin and a board of academic advisors, and funded by ChoicePoint Inc. (the "ORC survey").[56] The second survey was conducted in November 2000 by the Center for Survey Research and Analysis at the University of Connecticut, on behalf of the American Society of Newspaper Editors' Freedom of Information Committee and the First Amendment Center (the "ASNE survey").[57]

Despite the fact that both surveys report a high level of public angst about privacy—88% of respondents to the ORC survey report being concerned or very concerned about "misuse of personal information,"[58] and 89% of respondents to the ASNE survey report being concerned or very concerned about "personal privacy"[59] —both surveys show an equally high level of public support for keeping public records open.

In the ASNE survey, strong majorities of respondents believed that access to public records plays a "crucial role" in the functioning of good government (60%; 95% believed that access plays "some role");[60] 91% of respondents agreed with the statement "Even if I never need to view a public record myself, it is important that I have the right to do so."[61]

This support is by no means limited to access by journalists or public interest groups. The ORC survey asked respondents to indicate how important they found each of three justifications for accessible public records: government oversight by researchers and journalists, inquiries into government spending and policies by special interest groups, and facilitating economic transactions in the market. Sizeable majorities found all three important; almost three-fourths of respondents (73%) found access to public records for purely commercial purposes important.[62]

The ORC survey showed overwhelming support for commercial use of public records to locate parents to pay child support (96%); heirs, beneficiaries of insurance policies, and bank account holders (92%); and witnesses or parties to civil or criminal litigation (89%).[63] Support was similarly strong for commercial use of public records to do background checks on people working with children (96%) examine driving and accident records when checking insurance claims (89%); and check the bankruptcy history of potential vendors (82%).[64] The ORC survey also showed that the public overwhelming supports providing access to detailed personal information in public records to law enforcement officials (90%), employers making hiring decisions (83%), and businesses that provide consumer credit or insurance (74%).[65] Significantly, a majority of respondents supported every commercial use of public

record data that the ORC survey asked about, including access by private investigators (61%) [66] and "ordinary citizens like you" (53%).

CONCLUSION

Contrary to the misimpression created by the Subcommittee draft report, the Constitution does not prohibit public access to address and telephone information in public records. Quite the opposite, the Constitution permits and even encourages public access to such information. That fact, combined with the many valuable and beneficial uses of public record address and telephone data, highlights the practical and economic costs of eliminating public access to the information the government has spent tax dollars to collect. And it illuminates the magnitude of the interest that will have to be overcome for the State of New Jersey to demonstrate that closure is warranted.

Thank you.

Fred H. Cate is a Distinguished Professor at the Indiana University School of Law—Bloomington and founding director of Indiana University's Center for Applied Cybersecurity Research.

Professor Cate specializes in privacy, freedom of expression, and other information law issues. He is the author of many articles and books, including the award-winning *Privacy in the Information Age*, *Privacy in Perspective*, *The Privacy Problem: A Broader View of Information Privacy and the Costs and Consequences of Protecting It,* and *The Internet and the First Amendment*. He is the co-author of the sixth edition of *Mass Media Law* (with Marc Franklin and David Anderson).

He serves as the Reporter for the Department of Defense Technology and Privacy Advisory Committee, a Senior Policy Advisor to the Center for Information Privacy Leadership at Hunton & Williams, an Academic Advisor to the American Legislative Exchange Council, and a member of the Board of Editors of *Privacy and Information Law Report* and of the Microsoft Trustworthy Computing Academic Advisory Board.

Professor Cate directed the Electronic Information Privacy and Commerce Study for the Brookings Institution; chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities; served as vice chair of the American Bar Association Section on Health Law's Electronic Communications and Privacy Interest Group; and was a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. During the 2000 presidential race he advised the George W. Bush campaign on privacy matters.

He has testified on privacy issues before the Senate Committee on Banking, Housing, and Urban Affairs (2002); Senate Committee on Commerce, Science, and Transportation (2001); House Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection (2001); House Committee on Government Reform, Subcommittee on Government Management, Information and Technology (2000); House Committee on Banking and Financial Services, Subcommittee on Financial Institutions and Consumer Credit (1999); and House Committee on the Judiciary, Subcommittee on Courts and Intellectual Property (1998), as well as state legislative committees in California, Florida, Idaho, Indiana, and South Carolina.

Professor Cate received his J.D. and his A.B. with Honors and Distinction from Stanford University. He is a member of the Phi Beta Kappa Senate and of the Phi Beta Kappa Fellows Board of Directors, and he is listed in *Who's Who in America* and *Who's Who in American Law*. He may be contacted at:

Professor Fred H. Cate
Indiana University School of Law—Bloomington
211 S. Indiana Avenue
Bloomington, IN 47405
Tel (812) 855-1161
Fax (812) 855-0555
fcate@indiana.edu

Notes

---

[1]. Report of the Special Directive Subcommittee to the New Jersey Privacy Study Commission 24 (Sept. 8, 2003 draft).
[2]. Id. at 25.
[3]. Id. at 26-27.
[4]. Katz v. United States, 389 U.S. 347 (1967).
[5]. Griswold v. Connecticut, 381 U.S. 479 (1965).
[6]. Roe v. Wade, 410 U.S. 113 (1973).

[7]. Id. at 152-53.
[8]. Whalen v. Roe, 429 U.S. 589 (1977).
[9]. NAACP v. Alabama, 357 U.S. 449 (1958).
[10]. Stanley v. Georgia, 394 U.S. 557 (1969).
[11]. Rowan v. Post Office, 397 U.S. 728 (1970).
[12]. Federal Communications Commission v. Pacifica Foundation, 438 U.S. 726 (1978).
[13]. Frisby v. Schultz, 487 U.S. 474 (1988); Carey v. Brown, 447 U.S. 455 (1980).
[14]. 429 U.S. 589.
[15]. Id. at 599-600.
[16]. Id. at 603-04.
[17]. 142 N.J. 1, 84 (1995).
[18]. 170 F.3d 396 (3d Cir. 1999).
[19]. 227 F.3d 98 (3d Cir. 2000).
[20]. 341 F.3d 206 (3d Cir. 2003).
[21]. 638 F.2d 570 (3d Cir. 1980).
[22]. Smith v. Doe, 123 S. Ct. 1140 (2003).
[23]. 142 N.J. at 84.
[24]. Id. at 85.
[25]. 227 F.3d at 107 (emphasis added).
[26]. 341 F.3d at 211, 213.
[27]. 638 F.2d at 580-81.
[28]. Report of the Special Directive Subcommittee, supra at 7-8.
[29]. Daniel J. Solove, "Access and Aggregation: Public Records, Privacy and the Constitution," 86 *Minnesota Law Review* 1137 (2002).
[30]. 357 U.S. 449 (1958).
[31]. Id. at 462.
[32]. 988 F.2d 1344 (4th Cir. 1993).
[33]. 410 U.S. 113 (1973).
[34]. Solove, supra at 1203.
[35]. Pub. L. No. 103-322, 108 Stat. 1796 (1994) (codified at 18 U.S.C. §§ 2721-2725).
[36]. Condon v. Reno, 155 F.3d 453, 464 (4th Cir. 1998), rev'd on other grounds, Reno v. Condon, 528 U.S. 441 (2000) (emphasis added).
[37]. Id. at 465.
[38]. Id.
[39]. Reno v. Condon, 528 U.S. 441 (2000).
[40]. U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 528 U.S. 1188 (2000).
[41]. Id. at 1235 (quoting Rubin v. Coors Brewing Co., 514 U.S. 476, 486 (1995)).
[42]. Id.
[43]. Id., quoting Cincinnati v. Discovery Network, Inc., 507 U.S. 410, 417 (1993), and 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 529 (1996) (O'Connor, J., concurring) (citations omitted).
[44]. U.S. West, Inc. v. FCC, 182 F.3d 1224, 1235 (10th Cir. 1999), cert. denied, 528 U.S. 1188 (2000) (emphasis added).
[45]. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Terry v. Ohio, 392 U.S. 1, 9 (1968); Smith v. Maryland, 442 U.S. 735, 740 (1979).
[46]. Restatement (Second) of Torts ' 652A (1976).
[47]. See, e.g., Florida Star v. B.J.F., 491 U.S. 524 (1989).
[48]. 532 U.S. 514 (2001).
[49]. Id at 534, 121 S. Ct. at 1765 (quoting Time, Inc. v. Hill, 385 U.S. 374, 388 (1967) (quoting Thornhill v. Alabama, 310 U.S. 88, 102 (1940))).
[50]. Brooke Barnett, "Use of Public Record Databases in Newspaper and Television Newsrooms,"53 *Federal Communications Law Journal* 557 (2001) (emphasis added).
[51]. Hearings before the Committee on Banking and Financial Services, U.S. House of Representatives, July 28, 1998, (statement of Robert Glass, Vice President and General Manager of the Nexis Business Information Group of Lexis-Nexis).
[52]. See http://www.choicepoint.net/choicepoint/productwebdisplay.nsf/Child?openform.
[53]. Hearings before the Subcomm. for the Departments of Commerce, Justice, and State, the Judiciary and

Related Agencies of the Comm. on Appropriations, U.S. Senate, March 24, 1999 (statement of Louis J. Freeh).
[54]. "Address Endorsements Don't Always Work and That Costs You Cash," *Mail Center Management Report*, July 2001, at 1.
[55]. Robert E. Litan, "Balancing Costs and Benefits of New Privacy Mandates," 6 *Telecommunications & Space Journal* 115, 125 (1999).
[56]. ORC International and Alan F. Westin, *2000 ChoicePoint Public Opinion Survey* (2000). The survey involved telephone interviews with a national scientific sample of 1,011 adults, conducted in September and October 2000.
[57]. ASNE Freedom of Information Committee and the First Amendment Center, *Freedom of Information in the Digital Age* 19 (2001). The survey involved telephone interviews with a national scientific sample of 1,005 adults, conducted in November 2000. Both surveys have a margin of sampling error of plus or minus 3% at the 95% confidence level.
[58]. ORC Survey, supra at 31.
[59]. ASNE Survey, supra at 15.
[60]. ASNE Survey, supra at 16.
[61]. Id. at 18.
[62]. ORC Survey, supra at 27.
[63]. Id. at 37.
[64]. Id. at 45.
[65]. Id. at 53.
[66]. Id.