No. 01-729

IN THE
Supreme Court of the United States

GLENN G. GODFREY AND BRUCE M. BOTELHO,
Petitioners,
v.
JOHN DOE I, ET AL.
Respondents.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

BRIEF OF AMICUS CURIAE ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF DOE I, ET AL., Respondents

MARC ROTENBERG
Counsel of Record
MIKAL J. CONDON
ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Ave., NW,
Suite 200
Washington, DC 20009
(202) 483-1140

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE AMICUS CURIAE

Amicus the Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. that was established to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.[1] EPIC has participated as *amicus curiae* in numerous privacy cases, including most recently *Watchtower Bible and Tract Soc'y of N.Y., Inc. v. Vill. of Stratton*, 122 S. Ct. 2080 (2002). EPIC believes that the invasion of privacy imposed by the Alaska Megan's Law statute, which compels the collection of stigmatizing information and mandates its electronic dissemination, is grossly excessive in light of the statute's purpose.

SUMMARY OF THE ARGUMENT

The Alaska Megan's Law statute permits internet dissemination of stigmatizing information collected from released offenders by the state by mandating that the information in the registry be available "for any purpose … to any person."[2] Because government posting of registry

---

[1] Letters of consent to the filing of this brief have been lodged with the Clerk of the Court pursuant to Rule 37.3. Pursuant to Rule 37.6, amicus states that the counsel for amicus authored the brief with the assistance of law students Sara Rose and Jason Young, and PhD student Nicole Anastasopoulos, and that no monetary contributions were made for the preparation or submission of the brief.

[2] Alaska Sex Offender Registration Act (ASORA), Alaska Stat. § 12.62.010 (1999). In its implementing regulations, Alaska provides that it will, in all cases, "provide information in the central registry … for any purpose, to any person, without charge, by posting or otherwise making it available for public viewing in printed or electronic form." Alaska Admin. Code tit. 13, § 09.050(a) (2000).

information makes this information widely available to individuals not living in geographic proximity to the registrant, the punishment imposed by the statute is excessive.

Where the government compiles private information about an individual, the individual has a valid expectation that the information will not be disseminated indiscriminately. This privacy interest is particularly important today, when information that would otherwise be effectively unavailable is made readily accessible worldwide. Therefore, the government has a duty to impose safeguards and limitations upon its dissemination of such information. This duty can be met by using the principles laid out by the Code of Fair Information Practices to articulate a Megan's Law statute that creates an appropriate balance between the state's interest in protecting its citizens from recidivism and protecting the registrants' privacy interests.

ARGUMENT

I. Megan's Law Statutes Which Permit Registry Dissemination on the Internet Are Excessively Invasive of the Privacy of Released Offenders

Sex offender statutes, based on a particular community's right to know about the presence of sex offenders, do not categorically trump the privacy rights of released sex offenders. Community notification presents the issue of whether actively publicizing the names and criminal histories of released sex offenders violates the right to be free from unwanted disclosure of personal information. Privacy—a right inherent in the Constitution—in the context of released sexual offenders represents a "right to remain anonymous as against their neighbors." Alan R. Kabat, *Scarlet Letter Sex Offender Databases and Community Notification: Sacrificing Personal Privacy for a Symbol's*

Sake, 35 AM. CRIM. L. REV. 333, 337 (1998). Although society finds it acceptable to limit the privacy rights of criminals—as demonstrated by the public nature of criminal proceedings and records—sex offender registries should be subject to certain restrictions so that they are no more invasive than necessary to achieve the state's compelling purpose in collecting such information.

The Alaska statute, Alaska Sex Offender Registration Act (ASORA), Alaska Stat. § 12.62.010 (1999), was challenged as a violation of the Ex Post Facto Clause, U. S. Const. Art. I, § 10, for failure to provide fair notice and restrain arbitrary and potentially vindictive legislation. *Doe v. Otte*, 259 F.3d 979 (9th Cir. 2001), *cert. granted*, 122 S. Ct. 1062 (2002) (No. 01-729). Whether a criminal statute violates the Ex Post Facto Clause is a two step-inquiry established in *Kennedy v. Mendoza-Martinez,* 372 U.S. 144 (1963): (1) is the intent of the statute punitive, and (2) are there any punitive effects of the statute? The seventh factor weighed by the Court in determining punitive effect is whether the sanctions appear excessive in relation to the alternative, non-punitive, purpose of the statute. Under this test, placing sex offender registries on-line—where individuals not living in geographical proximity to the registrant could access the information—is excessive, and outweighs the state's compelling interest in protecting its citizens from a perceived threat of recidivism. The Court should find that where a Megan's Law statute mandates internet dissemination of a sex offender registry, the sanctions are disproportionately excessive under the *Mendoza-Martinez* inquiry.

A. Registrants Have a Protectable Privacy Interest in the Information Disseminated under ASORA

Access to public information such as law enforcement data is a tradition important to American open government;

however, the Court has indicated that a distinction should be made between information that is generally available to the public and compilations of information. Release of the latter—that implicated by dissemination of community notification information—raises questions of privacy that are not present in the former.

In *United States Dep't of Justice v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 756 (1989), the Court interpreted a provision of the federal Freedom of Information Act (FOIA) that exempted from mandatory disclosure "records or information compiled for law enforcement purposes, 'but only to the extent that the production of such materials . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy.'" The issue was whether disclosure of the contents of an FBI "rap sheet" on a member of an organized crime family constituted the type of personal privacy invasion protected by the FOIA exemption.

A unanimous Court determined that disclosure of the rap sheet implicated the interest "in avoiding disclosure of personal matters." *Reporters Comm.*, 489 U.S. at 762. The subject's privacy interest did not disappear simply because information in the report had previously been available to the public. The Court recognized that the power of the whole (the disseminated compilation) is greater than the sum of its parts (the individual information available to the public): "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *Reporters Comm.*, 489 U.S. at 764. Although *Reporters Committee* concerned an application of FOIA, the decision demonstrates that an individual can claim a privacy interest in compilations containing information that may exist in scattered pieces of public information. This privacy interest is greatly affected in

today's society where a "computer can accumulate and store information that would otherwise have surely been forgotten long before." *Reporters Comm.*, 489 U.S. at 771.

When applied to community notification, this distinction implies that offenders have a right to personal privacy with regard to government-maintained compilations that may not necessarily be present with regard to traditional criminal records. Registrants have a right to expect that information compiled by the government for a specific and limited purpose will not be randomly and widely disseminated inconsistent with the statutory purpose. *See* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy, and the Constitution*, 86 MINN. L. REV. 1137, 1195 (forthcoming 2002). This is especially true where the government has compelled the collection of stigmatizing information and promoted its pervasive dissemination. Although the public may have access to the information contained within sex offender registries, the privacy violation is greater when the government compiles the information and then takes steps to widely release it.

The Court subsequently applied the *Reporters Committee* reasoning to again find that an individual still has a privacy interest in information disseminated by the government despite the fact that the information may be obtained from public sources. *See Dep't of Defense v. Fed. Labor Relations Auth.*, 510 U.S. 487, 496-500 (1997). The Court recognized that, although federal employees' home addresses were publicly available in sources such as telephone books and voter registries, a federal agency's disclosure of the addresses to third parties would unjustifiably invade the employees' privacy: "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." *Fed. Labor Relations Auth.*, 510 U.S. at 500. As with rap sheets and compilations of home addresses of federal

employees, sex offender community notification provisions make publicly available a collection of information that, for practical purposes, would not be otherwise available. The mere fact that much of the information is available as part of the public record does not negate the expectations of released offenders that it will not be compiled and publicly disseminated by the state:

> In fact, the Constitution … also establishes certain responsibilities for the way that the government uses the information it collects. … [T]he fear of disclosure of personal information collected by the government is a recognized injury, one that can interfere with the exercise of fundamental rights.

Solove, 86 MINN. L. REV. at 1204.

Registration statutes that have survived Constitutional scrutiny have adopted different approaches to both the content and the dissemination of information. Some statutes—such as the Washington statute upheld by the Ninth Circuit—have very limited disclosure listing only the name and vicinity of the registrant rather than an exact address, while others—such as the New Jersey statute upheld by the Second Circuit—tier the registrants based upon post-conviction analyses of the individuals, and release information according to the risk of recidivism. *Compare* Wash. Rev. Code § 9A.44.130, upheld by *Russell v. Gregoire*, 124 F.3d 1079, 1082 (9th Cir. 1997), *with* N.J. Stat. Ann. § 2c:7-1 *et seq*., upheld by *E.B. v. Verniero*, 119 F.3d 1077, 1098 (3d Cir. 1997). Both types of notification fulfill the stated intent of registry statutes: to protect citizens from the possibility that the registered sex offender might re-offend, while limiting the invasion of the registrant's privacy. Where the information is not limited and permits access to more than those in immediate geographical proximity to the

individual, as is the case under ASORA, notification schemes do not create an acceptably narrow balance between the public's right to information and the registrant's right to privacy.

B. Widespread Dissemination of Stigmatizing Information Implicates Privacy Concerns

The government does not have unfettered discretion to publish the information it compiles from released sexual offenders. Although the state may disclose some information, offenders are entitled to a measure of protection before the government widely disseminates information about their pasts by posting the information on the internet.

The Court should uphold the Ninth Circuit's recognition that "[b]roadcasting the information about all past sex offenders on the internet does not in any way limit its dissemination to those to whom the particular offender may be of concern." *Otte*, 259 F.3d at 992. Because placing sex offender registries on-line is grossly excessive when weighed against the statutory purpose, such registries have an unconstitutionally punitive effect.

The Tenth Circuit, in *Femedeer v. Haun*, 227 F.3d 1244 (10th Cir. 2000), failed to consider the practical effects of such widespread dissemination of the registry upon those required to register, when analyzing the effect of internet dissemination of a Megan's Law registry under the seventh factor of the *Mendoza-Martinez* test. The court found that internet publication did not work an affirmative disability or restraint on convicted sex offenders because the information in the registry was merely an extension of the "public indictment, public trial, and public imposition of sentence, all of which necessarily entail public dissemination of information about the alleged activities of the accused." *Femedeer*, 227 F.3d at1251. The unlimited access provided by placing the registry on the internet, the Tenth Circuit

concluded, did not make the information any more public. The court wrote further that "[i]nterested individuals must still make an affirmative effort to retrieve the information [on the registry]," thus, "internet notification works merely a technological extension, not a sea change, in our nation's long history of making information public regarding criminal offenses." *Femedeer*, 227 F.3d at 1251.

The Tenth Circuit's position—that the inclusion of sex offender registries on the internet is no more than an extension of an already public record—completely fails to account for the increased privacy invasion caused by internet dissemination of such information. "[T]he Internet provides a much greater ability to aggregate and consolidate information." Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1409 (2001). The registry contains information the public records do not.[3] Additionally, this position permits those who do not live in that area to view and use the information for reasons unrelated to the statutory purpose.

The Court has previously described the unique nature of the internet in permitting access to otherwise effectively unavailable information:

> Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. … Taken

[3] For example, the Utah statute upheld by the Tenth Circuit included, in addition to the registrant's identifying information, a description of the individual's vehicle, method of offense, and common targets. *Femedeer*, 227 F.3d at 1250. ASORA requires basic information such as name and address, the vehicle identification number or any car to which the registrant has access (which includes all family cars), employer address, and information regarding any mental health treatment the registrant received since release. ASORA, Alaska Stat. § 12.62.010; *Otte*, 259 F.3d at 984, 987.

> together, these tools constitute a unique medium—known to its users as "cyberspace"—located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet. … The Web is thus comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services.

Reno v. ACLU, 521 U.S. 844, 851 (1997). Because of the uniquely ubiquitous nature of the internet, any negative effects of government regulation—such as invasion of privacy—are magnified. *See Reno,* 521 U.S. at 863 (approving the conclusion of the district court that the unique nature of the internet aggravated the vagueness of the statute).

The *Mendoza-Martinez* test requires the Court to balance the sanction imposed against the purpose of the statute. Because the internet provides unprecedented access to vast amounts of information, worldwide dissemination of the registrant's criminal history is clearly excessive in relation to the state's purpose of protecting local citizens from potential harm.

II. Safeguards are Necessary to Prevent Unwarranted Disclosure of Information Collected by the Government

The Court has recognized that certain safeguards are necessary to guard from privacy-invasive dissemination of information collected by the government. In *Whalen v. Roe*, the Court determined that the collection of prescriptions of addictive medications, required by state statute, was

adequately protected from unnecessary disclosure. However, the Court added:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. … The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. … We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data - whether intentional or unintentional - or by a system that did not contain comparable security provisions.

Whalen v. Roe, 429 U.S. 589, 605-06 (1977). As the Court recognizes, procedures must be in place to prevent unwarranted disclosure of personal information collected by the government—even information collected for a compelling government interest (as was the case in *Whalen* and is the case here). Therefore, safeguards must be put in place to ensure that government dissemination of sex offender registries does not unnecessarily infringe upon registrant's privacy rights.

The same issue has been debated in the context of placing public records on-line. Though EPIC is a strong advocate of open government, the organization has long recognized that the widespread dissemination of sensitive information within such records can present serious threats to individual privacy. *See generally* EPIC's Public Records Page, http://www.epic.org/privacy/public_records.html. "Government agencies have begun to place records on their websites, and public records, once physically scattered across

the country, can now be searched or gathered from anywhere in the country." *Solove*, 53 STAN. L. REV. at 1409. As one scholar noted:

> Privacy involves an expectation of a certain degree of accessibility of information. … [P]rivacy entails control over and limitations on certain uses of information, even if the information is not concealed. Privacy can be violated by altering levels of accessibility, by taking obscure facts and making them widely accessible.

Solove, 86 Minn. L. Rev. at 1178.

Publication of government documents, although important to provide public access to government activities, can represent serious threats to individual privacy when made available without use restrictions. The harms posed in the context of widely disseminated public records have been identified as including increased commercial profiling, predatory targeting,[4] false identification, public or private discrimination, identity fraud, pretexting,[5] and obliteration of

---

[4] The Federal Trade Commission filed a complaint in 2001 against companies targeting consumers considered to be greater credit risks and using deceptive marketing to encourage them to refinance debts at high interest rates and purchase high-cost credit insurance. *Fed. Trade Comm'n. v. Citigroup, Inc.*, No. 1:01-CV-606-JTC (N.D. Ga. Dec. 27, 2001). In Florida, a state representative proposed legislation to block the public release of police accident reports following allegations of automobile repair shop owners aggressively marketing their services to accident victims. Alan Judd, *Privacy vs. Public Access: Which Should Prevail?*, SARASOTA HERALD-TRIB., Nov. 2, 1997, at 1F.

[5] For example, 22 year old Amy Boyer was stalked and killed in New Hampshire after a women hired by a private investigator's service, Docusearch, used "pretexting" to obtain her work address. Docusearch obtained Boyer's work address by having a subcontractor, Michelle

social forgiveness. *See e.g.*, *Solove*, 86 Minn. L. Rev. at 1138 ("imagine the ease with which [personal] information could fall into the hands of crafty criminals, identity thieves, stalkers, and others who could use the information to threaten or intimidate individuals").

The harms posed by widespread dissemination of sexual offender records are more specific, and include vigilantism resulting in harm to the offender or harm to innocent third parties mistaken as the offender. *See, e.g.*, Kabat, 35 AM. CRIM. L. REV. at 340. While the Ninth Circuit recognized that hostility from the registrant's community might result from internet dissemination,[6] the use of this information by national groups that wish to target those convicted of sex offenses was not addressed. There have been well-documented examples of vigilante violence taken towards Megan's Law registrants. *See, e.g.*, Megan's Law -

---

Gambino, place a call to Boyer. Gambino lied about who she was and the purpose of her call in order to convince Boyer to reveal her employment information--Gambino pretended to be affiliated with Boyer's insurance company, and requested "verification" of Boyer's work address in order to facilitate an overpayment refund. *Remsburg v. Docusearch*, No. 00-211-B (Apr. 25, 2002) (Order of Certification).

[6] One of the plaintiffs in this case suffered community hostility and damage to his business after printouts from the Alaska sex offender internet website were publicly distributed and posted on bulletin boards. *Otte*, 259 F.3d at 988. The Ninth Circuit expressed concern that the employability of registrants in the future would be affected by similar behavior. *Otte*, 259 F.3d at 988.

Not only does listing in such a registry jeopardize the privacy rights of the registrant, members of that person's family are also affected. One of the plaintiffs in this case is the wife of an individual required to register who fears her reputation as a nurse would be affected by a listing which would include her husband's name, her address, and even a description of vehicles driven by members of her household. One can easily see that the adverse effect on the registrant's family may also extend to the registrant's children.

Part IV: Fear and Vigilantism *at* http://incestabuse.about.com/library/weekly/aa082597.htm (Aug. 08, 1997).[7] It is possible—and indeed likely—that there is an increased potential for harm threatened by widespread dissemination of personal information about someone inspiring intense emotions (as do convicted child sex offenders). Such danger was evidenced following the posting of the Nuremburg Files, a website providing a list of abortion doctors with personal information in a manner that some have considered tantamount to a hit list. *See* John P. Cronan, *Free Speech on the Internet: Does the First Amendment Protect the "Nuremburg Files"?*, 2 YALE L. & TECH. 5, http://lawtech.law.yale.edu/symposium/00/comment-cronan.htm (2000); *Solove*, 86 MINN. L. REV. at 1189; *cf. Zeran v. Diamond Broadcasting, Inc.*, 203 F.3d 714, 717 (10th Cir. 2000) (following an anonymous posting on an internet bulletin board wrongfully accusing Zeran of profiting from the 1995 Oklahoma City bombings, Zeran received numerous "nasty and threatening" phone calls and death threats). Furthermore, placing information about an individual's criminal history on the internet increases the threat of negative profiling resulting in total destruction of social forgiveness,[8] and the possibility of data entry error.[9]

---

[7] For example, upon release of register information, registrants have had their cars fire-bombed, their homes broken into, and have been assaulted, stalked, and harassed. Megan's Law - Part IV: Fear and Vigilantism *at* http://incestabuse.about.com/library/weekly/aa082597.htm (Aug. 08, 1997).

[8] "Social forgiveness" is the principle that over time a citizen's crimes are forgiven by society, that "[h]uman forgetfulness over time puts today's 'hot' news in tomorrow's dusty archives. In a nation of 200 million people there is ample opportunity for all but the most infamous to begin a new life." *Briscoe v. Reader's Digest*, 483 P.2d 34 (Cal. 1971). However, while individuals may petition a court to expunge a criminal record, if a notation of the crime exists in an on-line database, the individual may still be marked as a criminal by profiling companies or employers, and thus,

The District Court of New Jersey addressed a Megan's Law statute providing for internet dissemination of the offender registry. Applying the same test used by the Ninth Circuit, the court held that the widespread dissemination of information about the offenders is more broad than necessary to meet the government's interest in protecting those who might encounter the offender, because "[t]he proposed Internet registry, … *dispenses with any safeguards designed to carefully limit disclosure of protected information* to individuals and groups with a legitimate public safety-related need for the information." *A.A. v. New Jersey*, 176 F. Supp. 2d 274, 302 (D.C.N.J. 2001) (emphasis added). As the court noted:

> in making the home addresses of a subset of Megan's law registrants available to the general public via the Internet, the Act also permits access to this information by people who will never actually encounter any registered sex offenders in New Jersey nor have any particular need for the information.

---

the chances of social forgiveness become lessened as the social recollection of the crime is increased.

[9] *See, e.g.*, Eugene Meyer, *Md. Woman Caught in Wrong Net; Data Errors Link Her To Probes, Cost 3 Jobs*, WASH. POST, Dec. 15, 1997, at C1 (woman's name, date of birth and Social Security number entered in connection with four child protective services cases in error and not corrected for 12 years); Julie Hairston, *Atlanta Police Technology Falls Short*, ATLANTA JOURNAL-CONSTITUTION, Aug. 2, 1998, at C1 (quoting Atlanta Corrections Commissioner describing how Atlanta's Criminal Justice Information System magnifies data entry errors as records move through the system: "We just had an unacceptable rate of inaccurate entries. We've essentially corrected that, but these are still human beings who are entering the data."); Gareth Walsh, *Court Order Causes Reporter Concern - Liability Order Wrongly Issued*, NEWCASTLE JOURNAL, Mar. 25, 1999, at 12 (computer error leads to court order being issued wrongly against innocent person).

> In doing so, *the Act impermissibly strips this protected information of any protection from unnecessary public disclosure*.

A.A., 176 F. Supp. 2d at 302-03 (emphasis added). While some public records are useful to individuals outside the immediate area where those records are made available in a more limited manner, there is little support for the argument that the type of information maintained in sex offender registries is of any use to individuals outside of the area where a potential risk of harm from the registrant exists.[10] Sex offender registries should focus on allowing citizens to track potential harm in their communities as opposed to tracking specific registered individuals; thus, internet access to these particular public records has little connection to the stated rationale for compiling such records in the first place.

Internet dissemination of such information permits the government to make unfettered use of information that would otherwise be effectively unavailable, violating the duty—imposed by the Court in cases such as *Reporters Committee* and *Whalen*—to safeguard private information from unwarranted disclosure.

---

[10] Narrower methods exist for making such information available for limited purposes, such as for someone considering moving to a particular area or neighborhood who is interested in statistics regarding local sex offenders. Such methods might include an internet registry that posts general area—but not name or address—of registered offenders, or a provision permitting individualized remote requests to local police stations via mail or facsimile. *See, e.g.*, Reuters, *L.A. to Track Sex Offenders on Internet*, July 30, 2002, http://story.news.yahoo.com/news ?tmpl=story&u= /nm/20020731/wr_nm/crime_map_dc_2.

III. A Megan's Law Statute that Provides a Better Balance of the Safety Interests of the Public and the Privacy Interests of the Registrant is Feasible

A sex offender statute that properly balances the interests of the public and the registered sex offender can be created by drafting a law based upon the Code of Fair Information Practices. *See* Kabat, 35 AM. CRIM. L. REV. at 354-56, citing to U.S. Dep't. of Health, Education and Welfare, *Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens viii* (1973).[11] Using the Fair Information Practices as a model, at least one theory for a valid database notification law has been advanced, which suggests that a valid Megan's Law statute can be created by providing the following:

1. *Openness*: making the existence of the database known to all relevant parties;
2. *Duration*: defining a reasonable time during which the registrant will remain in the database if the individual commits no further violation, after which the individual's information will be purged from the database;
3. *Collection Limitation*: the scope of information collection must be clearly defined in terms of the information sources;

[11] For a discussion of the development of Fair Information Practices, see David E. Flaherty, *Protecting Privacy in Surveillance Societies* 352-53 (1989), and Dan Solove and Marc Rotenberg, *Information Privacy Law* (forthcoming Aspen 2002).

4. *Purpose Specification*: the database must clearly delineate its purpose with a direct limitation of use based upon that purpose;
5. *Individual Participation*: the registrant must be allowed to review and correct his or her own records in the database;
6. *Data Quality*: there must be procedures in place to ensure the accuracy of listed information;
7. *Use Limitation*: The geographic and organizational scope of disclosure must be clearly defined; and
8. *Security Safeguards*: there must be mechanisms in place to protect the information in the databases.

See Kabat, 35 AM. CRIM. L. REV. at 354-56. A particular use limitation that would address the concerns of the Ninth Circuit would be to provide only general information about where registrants live on-line, while requiring residents to go to a police station to get the actual addresses, photos and criminal histories of offenders. Such a system has been implemented in various parts of California, where state law prohibits the release of the entire registry over the internet. *See L.A. to Track Sex Offenders on Internet*, *supra*, note 5.

If weighed under the *Mendoza-Martinez* test, a statute carefully crafted under Fair Information Practice principles would survive *Mendoza-Martinez* scrutiny because it would address the particular concerns properly expressed by the Ninth Circuit that such a statute authorize the release only of "relevant and necessary information" within "a 'narrow geographic area.'" Otte, 259 F.3d at 992, quoting *Russell*, 124 F.3d at 1082. In particular, the concept of "use limitation" provides for better protection of the privacy interests of the registrants by safeguarding unwarranted disclosures, a concern expressed by the Court in *Whalen* and

Reporters Committee. In this circumstance, the government would be limited to localized publication, thereby fulfilling the purpose of the statute without unnecessarily infringing upon the registrants' privacy rights.

CONCLUSION

Respondents have a privacy right in the information collected and disseminated by the ASORA. Although the state has a compelling reason for collecting and making available the information in limited circumstances, internet dissemination of such information permits the government to make unfettered use of information that would otherwise be effectively unavailable, thus violating the state's duty to safeguard private information from unwarranted disclosure. The decision of the Ninth Circuit should therefore be affirmed for the reasons stated herein.

Dated: August 2, 2002

Respectfully submitted,

MARC ROTENBERG
Counsel of Record
MIKAL J. CONDON
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Ave., NW, Suite 200
Washington, DC 20009
(202) 483-1140