JAMES KEHOE,

Plaintiff-Appellant,

vs.

FIDELITY FEDERAL BANK AND TRUST,

Defendant-Appellee.

No. 04-13306-BB

IN THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

BRIEF OF AMICI CURIAE ELECTRONIC PRIVACY INFORMATION CENTER AND AMERICAN CIVIL LIBERTIES UNION OF FLORIDA IN SUPPORT OF PLAINTIFF-APPELLANT, URGING REVERSAL

STATEMENT OF AMICI CURIAE

Pursuant to Rule 29 of the Federal Rules of Appellate Procedure, this brief is respectfully submitted by the Electronic Privacy Information Center ("EPIC"). Plaintiff-Appellant has consented to the filing of this brief; Defendant-Appellee does not consent to the filing of this brief. Consistent with FRAP 29, *Amici* have filed a motion accompanying this brief seeking leave from this Court to file.

EPIC is a not-for-profit public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC is a leading national advocate on privacy issues, and its Advisory Board and staff members possess expertise on the commercial use of personal information. EPIC maintains a detailed Web site on privacy online at http://epic.org/.

The American Civil Liberties Union ("ACLU") is a nationwide nonpartisan organization of nearly 400,000 members dedicated to protecting the fundamental liberties and basic civil rights guaranteed by the state and federal Constitutions. The ACLU of Florida is its state affiliate and has approximately 22,000 members in the State of Florida also dedicated to the principles of liberty and equality embodied in the United States Constitution and the Florida Constitution. The ACLU has a long standing interest in protecting the privacy rights of individuals. In 2003, the ACLU of Florida brought Florida's non-compliance with the DPPA to the attention of the United States Attorney General and called upon the Governor to support legislation to bring Florida into compliance.[1] The proper resolution of this case is therefore a matter of substantial concern to the ACLU of Florida and its members.

STATEMENT OF THE ISSUE

Did the court below err in ruling that the DPPA requires a plaintiff to show actual damages before being awarded liquidated damages in light of Congressional intent to protect individuals both from actual harm and from risk presented by the indiscriminate sale of personal information by the government?

SUMMARY OF ARGUMENT

At issue in this case is whether a plaintiff suing under the Drivers Privacy Protection Act ("DPPA") for an intentional violation of the Act must show actual damages in order to recover liquidated statutory damages of $2,500.

The DPPA is one part of a patchwork of privacy laws that shield personal information from disclosure. In passing the DPPA, Congress added provisions to the criminal code to prevent governmental entities from releasing personal information indiscriminately, as such release has led to documented stalking, robbery, and murder.

The court below relied upon the recently decided case in *Doe v. Chao*, where the Supreme Court held that the Privacy Act requires a showing of actual damages before a plaintiff can recover liquidated damages. *Doe* should not control this case because the plain language of the DPPA differs from the Privacy Act; because statutory interpretation tools employed by the lower court lead to illogical consequences; because unlike the Privacy Act, Congress did not weaken damages provisions from the DPPA in the process of enacting it; and because there is no risk that the federal fisc will be depleted from an award of liquidated damages under the DPPA.

The DPPA is also different in context than the Privacy Act. The Privacy Act operates within a larger framework of laws that promote government accountability. The DPPA, on the other hand, is one of the few tools available to protect personal information from unaccountable commercial entities, like the Appellee in this case, that routinely seek access to personal information in government records. Without liquidated damages provisions, some unscrupulous actors may continue to access motor vehicle records for private investigation, commercial marketing, or other purposes.

The DPPA's liquidated damages provisions are critical to the prevention of physical harms and the risks associated by the release of personal information generally. Without liquidated damages, an individual whose personal information was purchased by a stalker or potential attacker would not be entitled to recovery until they were actually harmed.

The legislative history of the DPPA demonstrates that Congress intended the law to address both dangerous criminals and the general risk presented by sale of motor vehicle information to strangers. Liquidated damages were included in the DPPA to ensure that these harms and risks would be recoverable at law.

In a broader context, liquidated damages provisions are essential to the meaningful protection of information privacy. Information privacy violations are sometimes difficult to demonstrate and quantify. Liquidated damages provisions ensure compensation for the victim, deter future violations, and promote judicial economy.

We urge this Court to reverse the decision of the lower court and hold that a plaintiff who successfully proves that a person knowingly violated the DPPA is entitled to liquidated damages.

ARGUMENT

I. The Supreme Court's Decision in *Doe v. Chao*, Limiting Access to Liquidated Damages Under the Privacy Act, Should Not Control This Case

The Supreme Court relied upon a number of factors to hold that the Privacy Act[2] does not grant plaintiffs liquidated damages without a demonstration of actual harm in *Doe v. Chao* ("Doe").[3] The Drivers Privacy Protection Act ("DPPA")[4] is distinguishable from the Privacy Act, and accordingly, *Doe* should not control this case.

A. The Plain Language of the DPPA Differs from the Privacy Act.

The relevant section of the Privacy Act examined by the Supreme Court in *Doe* provides:

> (4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—
> (A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person *entitled to recovery* receive less than the sum of $1,000; [5]

The Supreme Court in *Doe* interprets this provision as barring any award of the statutory minimum without proof of actual damages. However, the Supreme Court's textual interpretation relies heavily on the phrase "entitled to recovery." In the Supreme Court's words:

> When the statute gets to the point of guaranteeing the $1,000 minimum, it not only has confined any eligibility to victims of adverse effects caused by intentional or willful actions, but has provided expressly for liability to such victims for "actual damages sustained." It has made specific provision, in other words, for what a victim within the limited class may recover. When the very next clause of the sentence containing the explicit provision guarantees $1,000 to a "person entitled to recovery," the simplest reading of that phrase looks back to the immediately preceding provision for recovering actual damages, which is also the Act's sole provision for recovering anything (as distinct from equitable relief). With such an obvious referent for "person entitled to recovery" in the plaintiff who sustains "actual damages," Doe's theory is immediately questionable in ignoring the "actual damages" language so directly at hand and instead looking for "a person entitled to recovery" in a separate part of the statute devoid of any mention either of recovery or of what might be recovered.[6]

The importance of this phrase is additionally reflected when, later in the opinion, the court terms the privacy damages provisions of another law (the Tax Reform Act) as, "(t)oo far different from the language of the Privacy Act to serve as any sound basis for analogy; it

does not include the critical limiting phrase 'entitled to recovery.'"[7]

But this "critical limiting phrase" is absent from the DPPA damages provision at issue in this case. The DPPA provides that, "(t)he court may award- (1) actual damages, but not less than liquidated damages in the amount of $2500."[8]

The District Court implicitly admits the weakness of its *Doe* analogy. The opinion notes "[Kehoe's argument] that since the DPPA does not contain the Privacy Act's language limiting the minimum statutory award to 'person(s) entitled to recovery,' the decision in *Doe* is inapposite to this case."[9] And in response to this noted argument, the court only offers the weak defense that, in addition to *Doe*, "the sum of several legal principles supports Fidelity's reading of the DPPA."[10]

Given the textual dissimilarities, the decision in *Doe* should not have controlled the interpretation of the DPPA. For this reason and for the reasons explained below, the error of the District Court's analogy is not assuaged by an assurance that, "the sum of several legal principles" supports the same reasoning.

B. Unlike the Privacy Act, the Relevant Damages Provision of the DPPA Presents no Risk to the Federal Fisc

The decision in *Doe* can be regarded as partly motivated by a feared "depletion of the federal fisc."[11] This fear is essentially characterized as a worry that every time the government makes a mistake in handling private information, it would suffer significant liability. But in this case, the specter of bankrupting the federal fisc is inapplicable, as the provision at issue is normally employed against persons or corporations who knowingly access motor vehicle records.[12]

C. The "Rule of Last Antecedent" Is Not Controlling Authority and When Applied Produces an Illogical Outcome

The District Court's interpretation of the text of the DPPA relies in part on the fact that,

> (U)nder the rule of last antecedent, "an accepted canon of statutory construction," "when considering statutes- qualifying words, phrases, and clauses are to be applied to the words or phrase immediately preceding, and are not to be construed as extending to including others more remote."…Under this rule, the qualifying language of "but not less than liquidated damages in the amount of $2500" would apply only to the phrase "actual damages" immediately preceding it, and would not extend out as its own remedy to be awarded regardless of actual damages.[13]

While it is true that courts have applied the rule of last antecedent in the past, they have also noted that the rule is not a controlling authority and should not be applied if it leads to illogical outcomes unsupported by other statutory interpretation tools. The Supreme Court recently commented that "this rule is not an absolute and can assuredly be overcome by other indicia of meaning."[14] In addition, scholars have in various papers noted that "the rule of last antecedent" is not an ideal interpretative tool.[15]

Since the rule of last antecedent is not dispositive, it should not be applied by this Court.

D. Unlike the Privacy Act, the Legislative History of the DPPA Does Not Indicate that Congress Removed Liquidated Damages Provisions

In *Doe*, the Supreme Court notes that a prior draft of the Privacy Act contained a provision for general damages and that this provision was ultimately omitted from the enacted version. The court treats this as an indication of the Congress' intent not to allow plaintiffs to recover general damages. The Supreme Court noted in *Doe* that:

> (D)rafting history show(s) that Congress cut out the very language in the bill that would have authorized any presumed damages. The Senate bill would have authorized an award of "actual and general damages sustained by any person," with that language followed by the guarantee that "in no case shall a person entitled to recovery receive less than the sum of $1,000…this language was trimmed from the final statute, subject to any later revision that might be recommended by the Commission. The deletion of "general damages" from the bill is fairly seen, then, as a deliberate elimination of any possibility of imputing harm and awarding presumed damages. The deletion thus precludes any hope of a sound interpretation of entitlement to recovery without reference to actual damages.[16]

The DPPA, unlike the Privacy Act, does not have a legislative history that "precludes any hope of a sound interpretation of entitlement to recovery without reference to actual damages." At no point in the DPPA's legislative history was any provision referencing general damages deleted. In fact, relevant legislative history indicates that Congress strengthened the DPPA and intended to provide general damages. As introduced in the House and Senate, the DPPA provided no private cause of action against violators.[17] As enacted, however, the DPPA provided a private right of action with a series of remedies, including liquidated damages for knowing violations of the Act.

E. Unlike the Privacy Act, The DPPA Directly Addresses Unaccountable Commercial Actors That Purchase and Sell Personal Information

The provision of the DPPA at issue addresses private investigators, private-sector "data brokers," and other politically unaccountable entities that obtain or sell personal information for a wide variety of purposes.[18] The DPPA is one of the only tools individuals possess to address commercial purchasers of personal information. Accordingly, preservation of a robust remedy is essential to making its protections meaningful.

The consequences of allowing liquidated damages under the DPPA differ from those associated with damages under the Privacy Act. The section of the Privacy Act interpreted in *Doe* provides a financial penalty to deter the United States government from violating privacy. This financial penalty operates in conjunction with many other checks that help keep the federal government accountable. The Privacy Act itself limits government disclosure of personal information, requires openness, accuracy, and accounting of disclosures.[19] But accountability also flows from elections, agency oversight by Congress, and open government laws that provide sunshine on federal activity.

These safeguards do not restrain commercial actors that trade in personal information. For instance, private investigators are a major concern of the DPPA and have obtained personal information for stalkers and murderers in the past.[20] But in some states, private

investigators are not even subject to licensure.[21] The DPPA is one of the only tools that individuals have to prevent private investigators from illegally accessing their motor vehicle records.

While Congress passed legislation in 1999 requiring States to adopt opt-in protections for motor vehicle records, Florida did not enact legislation implementing this requirement until this year.[22] As a result, commercial data brokers sell a number of automobile databases comprised of Florida residents that are not available on other states' residents. Five Florida-specific marketing databases exist offering for sale drivers' personal information, apparently drawn from Florida public registers.[23] These include databases marketed as "Florida's Exotic Automobiles," a database of "exotic automobiles registered in the State of Florida," and "Auto Insurance Individuals of Florida," which is drawn from "Controlled circ government records," and is comprised of "[v]ehicles registered to individuals in the state of Florida."[24] In the aggregate, the open marketing of these databases subjects Florida residents to many junk mail solicitations that would not be received in other states.

A narrow interpretation of the DPPA that does not award liquidated damages would create a risk that commercial data brokers will continue to acquire and resell personal information from motor vehicle records. Similarly, a private investigator might continue to access motor vehicle records unless there is a strong default punishment. Plaintiffs, unless they manufacture losses, face hurdles in showing that merely accessing the motor vehicle record or receiving junk mail constitutes an actionable harm. What people suffer from the unauthorized distribution of their private information is a privacy violation of a nature so elusive to quantify that it explains the DPPA's provision of a fixed minimum sum as appropriate compensation.

In essence, an interpretation of the DPPA based on *Doe* eliminates the deterrence effect of the DPPA's penalty provisions, and frees unscrupulous private actors to violate privacy in the comfort that few if any honest people would learn of the privacy violation and actually fall into the category of those with standing to recover damages.

II. Liquidated Damages Are Critical to Effecting Congress' Intent to Prevent Indiscriminate Sale of Personal Information

In enacting the DPPA, Congress was reacting to a series of serious crimes and threats of crimes caused by state governments that sold personal information from motor vehicle records indiscriminately. By placing the DPPA's protections in the criminal code, Congress sought to strongly deter the release of personal information and crimes facilitated by the flow of personal information.

Without liquidated damages, individuals would not be able to effectively deter sale of their information until it is too late—when information has been acquired and used to harm an individual. Congress also incorporated a liquidated damages clause to place a value on the harm caused by mere release of personal information, even where such release did not result in physical harm to an individual.

A. Congress Intended to Provide Liquidated Damages, Otherwise Some Victims Could Not Recover Until They Encountered An Attacker

The first indication of the intention to provide for minimum damages can be gleaned from

the nature of the event that spurred the DPPA's enactment—the stalking and murder of Rebecca Schaeffer, a young actor. Senator Boxer, an original sponsor of an unenacted version of the DPPA,[25] specifically invoked Schaeffer's murder when discussing the DPPA on the floor of the Senate:

> "I join the Senator from Virginia [Mr. Warner] and 26 other cosponsors, to offer an amendment to protect the privacy of all Americans. In California, actress Rebecca Schaeffer was brutally murdered in the doorway of her Los Angeles apartment by a man who had obtained her home address from my State's DMV…"[26]

The legislative history of the DPPA is rich with examples where government-held information was used to target victims of robberies, victims of murder, victims of stalking, and women who had visited health clinics.[27] These victims received no notice that their personal information was sold to an attacker. They might have known of the general risk created by the government's sale of personal information. But each suffered no physical or emotional harm until they encountered their attackers.

Under the District Court's interpretation of the law, obtaining Rebecca Schaeffer's address itself would not be remedied under the law. The only remedy would be when "actual damage" had occurred, *i.e.* when she was murdered. Congress did not intend this to be the result of its efforts to pass the DPPA. If Congress intended to prevent future occurrences like Ms. Schaeffer's murder as the record shows it did, then Congress must have intended to prevent the murder by limiting the mere sale of her personal information.

B. Mere Disclosure of Motor Vehicle Records Harms Individuals; Congress Sought to Ensure Recovery for This Harm Through Liquidated Damages

In addition to the risk of violent crime posed by the release of personal information, Members of both the Senate and the House of Representatives were concerned generally with the ease with which any person could gain access to driver information. That is, they were concerned with the per se harm and unease caused by easy access to government-maintained personal information. Senator Barbara Boxer noted in support of the DPPA that:

> In 34 States, someone can walk into a State Motor Vehicle Department with your license plate number and a few dollars and walk out with your name and home address. Think about this. You might have an unlisted phone number and address. But, someone can find your name or see your car, go to the DMV and obtain the very personal information that you may have taken painful steps to restrict.[28]

Senator John Warner spoke of the risks presented by indiscriminate release of driver information as well:

> I had no idea when I went into my State to get licensed that all this information that I provided was going to be made public...
>
> …this legislation is to protect a wide range of individuals, protect them from the State agencies often for a price, a profit to the State, to release lists. Not

> only will the agency give out individual names and sponsors will call with an inquiry, but they give out the whole list, everybody in the State, if you want to buy it…[29]

Senator Charles Robb, also a cosponsor of the unenacted version of the DPPA, expressed similar concerns and argued that government should not be endangering citizens through release of personal information. Like Senator Warner, Senator Robb expresses an objection to the mere disclosure of motor vehicle records:

> While this bill alone will not stop people from stalking, it will inhibit States from unknowingly aiding and abetting this type of crime. Easy access to personal information makes every driver in this Nation vulnerable and infringes on their right to privacy. Government's duty is to keep citizens safe and it should not, therefore, be contributing to insecurity...[30]

Senator Joseph Biden echoed Senator Robb's concerns:

> This amendment closes a loophole in the law that permits stalkers to obtain--on demand--private, personal information about their potential victims…
>
> Thus, potential criminals are able to obtain private, personal information about their victims simply by making a request. These open-record policies in many States are open invitations to would-be stalkers…
>
> The States should not provide the mechanism for the terror that can be unleashed through the indiscriminate release of this kind of information…[31]

In the House, Representative James Moran, a sponsor of unenacted companion legislation, [32] expressed an objection to access to personal information even where there is no resulting physical harm:

> "Random access to personal information contained in DMV files poses a threat to every licensed driver in the Nation…In Virginia, like most other States, licensees are not notified that their personal information has been accessed.[33]

Representative Moran also argued that:

> "(v)ery few people realize that anybody can write down the license plate number of your spouse and daughter and find out where they live and their name and their Social Security number in many States; it should not be allowed to continue."[34]

These statements in support of legislation to protect driver information encompass the harm caused by an unauthorized release of information even if there was no subsequent physical or economic damage. It is clear that accessing the information itself causes a cognizable harm in the minds of the DPPA's sponsors.

Because it is difficult to quantify harms caused by mere disclosure of personal information, these Members sought to ensure that this harm could be addressed at law by the inclusion of a liquidated damages clause. These Members intended to address ills that the lower court's

interpretation would leave unremedied.

III. Minimum Damages Clauses Serve An Essential Purpose in Information Privacy Laws of Addressing Unquantifiable Harm and Risk

Tort law has long provided remedies for intangible harms, such as those resulting from defamatory statements or torts against dignity.[35] A central problem in privacy cases is the difficulty for the injured party to demonstrate actual damages.[36] This problem was well understood by Samuel Warren and Louis Brandeis, the authors of the famous article that provided the basis for the privacy torts.[37]

Thus, in order to compensate the victim and recognize that a harm was committed, though it may be difficult to quantify, privacy statutes routinely include liquidated damage provisions. While the actual language providing statutory damages varies, there is no significant difference in the purpose.

Where there is an intentional violation of a privacy statute, awards of such damages ensure compensation for the victim, deter future violations, and promote judicial economy by reducing the need for difficult determination of harm in cases.

A. Privacy Scholars Recognize the Critical Role of Liquidated Damage Provisions in Privacy Statutes

The purpose of liquidated damages in privacy statutes is not only to compensate the victim for an intangible harm, but also to provide enforcement of such statutes.[38] Professor Jay Weiser has written that federal privacy statutes attempt to resolve the difficulty in calculating damages through liquidated damages provisions, which in turn saves enforcement costs.[39]

Liquidated damages are appropriate to address modern information privacy problems. Indiscriminate sale of personal data contributes to an "architecture of vulnerability"—the general availability of personal information places individuals at continuous risk of identity theft and privacy violations. George Washington University Law School Professor Daniel Solove has argued that this architecture of vulnerability is systemic and difficult to attribute to single forces or entities:

> They are the product of information flows, which occur between a variety of different entities. There is often no single wrongdoer; responsibility is spread among a multitude of actors, with a vast array of motives and aims, each doing different things at different times…The harm is created by the totality of privacy invasions, but [tort law] only focuses on each particular actor…
>
> Entities often buy and sell information, resulting in the disclosure of that information to only a few other entities. It is difficult to assess damages when one company maintains a database about a person and sells that information to other companies or the government. These harms do not translate well to tort law or criminal law, which focus on isolated actors and address harms individually rather than collectively." [40]

Because it is difficult to fit these harms into existing criminal or tort law, Solove argues,

Congress has incorporated minimum damages provisions into modern consumer protection laws to shield information privacy:

> Certain more modern privacy laws - namely, a number of the statutes passed since the 1970s - have minimum damages provisions, eliminating the difficult task of proving specific harm.[41]

Liquidated damage provisions also relieve juries of difficult damages determinations.[42] Thus, highly discretionary calculations are unnecessary. The purpose of statutory damages is both to encourage a victim to pursue a case under a privacy statute and to serve as a deterrent to would-be violators.[43]

CONCLUSION

For the foregoing reasons, Amicus Curiae Electronic Privacy Information Center urges this Court to reverse the decision of the U.S. District Court for the Southern District of Florida.

Dated: August 31, 2004

Respectfully submitted,

By:_____

Chris Jay Hoofnagle
Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
Telephone: **(202) 483-1140**

Attorney for Amicus Curiae Electronic Privacy Information Center

Randall C. Marshall
ACLU Foundation of Florida, Inc.
4500 Biscayne Boulevard - Suite 340
Miami, FL 33137-3227
(305) 576-2337
(305) 576-1106 (fax)

Attorney for Amicus Curiae ACLU of Florida

---

[1]American Civil Liberties Union of Florida, ACLU Asks Attorney General John Ashcroft to Enforce Driver's License Information Privacy Law in Florida, Apr. 8, 2003, *available at* http://www.aclufl.org/news_events/archive/2003/dlprivacy040803.cfm; American Civil Liberties Union, ACLU Urges Governor Bush To Support Legislation Protecting Privacy Rights of Florida Drivers, Apr. 18, 2003, *available at* http://www.aclufl.org/news_events/archive/2003/dppa.cfm.

[2] 5 U.S.C. § 552a (2004).

[3] *Doe v. Chao*, ___ U.S. ___, 124 S. Ct. 1204 (2004).

[4] 18 U.S.C. § 2721 et seq. (2004).

[5] 5 U.S.C. § 552a(g)(4)(A) (2004) (emphasis added).

[6] *Doe*, 124 S. Ct. at 1208.

[7] *Id*. at 1212.

[8] 18 U.S.C. § 2724(b) (2004).

[9] *Kehoe v. Fidelity Federal Bank and Trust*, Slip Op. at 8, No. 03-80593-Civ-Hurley/Lynch (S.D. Fla. 2004).

[10] *Id*.

[11] *Doe*, 124 S. Ct. at 1217 (Ginsburg, J. dissenting).

[12] States and state agencies are specifically excluded from persons liable under the DPPA. *See* 18 U.S.C. §§ 2724(a), 2725(2).

[13] *Kehoe v. Fidelity Federal Bank and Trust*, Slip Op. at 8, No. 03-80593-Civ-Hurley/Lynch (S.D. Fla. 2004) (emphasis added)(internal citations omitted).

[14] *Barnhart v. Thomas*, 540 U.S. 20, 124 S. Ct. 376, 380 (2003).

[15] *See, e.g.*, Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons about how Statutes are to be Construed*, 3 Vand. L. Rev. 395 (1950).

[16] *Doe* at 1209-10.

[17] Driver's Privacy Protection Act of 1993, H.R. 3365, 103rd Cong. § 2723 (1st Sess. 1993); Driver's Privacy Protection Act, S. 1589, 103rd Cong. § 2723 (1st Sess. 1993).

[18] *See, e.g.*, Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement*, 29 U.N.C. J. Intl. L. & Comm. Reg. 595 (Summer 2004) (describing the activities of commercial data brokers and arguing that the Privacy Act should apply to private companies that routinely sell personal information to the government).

[19] 5 U.S.C. § 552a (2004)

[20] 139 Cong. Rec. S15762 (Nov. 16, 1993)(statement of Sen. Boxer); *Remsburg v. Docusearch, Inc.*, 149 N.H. 148 (N.H. 2003)(private investigator and Florida data broker defendants sold personal information of woman to her stalker/killer).

[21] "Some States have few requirements [for private investigator licensure], and 6 States—

Alabama, Alaska, Colorado, Idaho, Mississippi, and South Dakota—have no statewide licensing requirements while others have stringent regulations." U.S. Department of Labor, Bureau of Justice Statistics, Private Detectives and Investigators, Mar. 21, 2004, available at http://www.bls.gov/oco/ocos157.htm (last visited Aug. 16, 2004).

[22] *Kehoe v. Fidelity Federal Bank and Trust*, No. 03-80593-Civ-Hurley/Lynch (S.D. Fla. 2004); Fla. Stat. § 119.07(3)(aa)(12) (2003); Fla. House Bill 1737, 2004 Fla. 62.

[23]SRDS, 37 Direct Marketing List Source 1379-1400 (Feb. 2003).

[24] *Id*. at 1381, 1389; Electronic Privacy Information Center, Kehoe v. Fidelity Federal Bank and Trust Page (Aug. 2004), available at http://www.epic.org/privacy/drivers/kehoe.html (last visited Aug. 16, 2004).

[25] Driver's Privacy Protection Act, S. 1589, 103rd Cong. (1st Sess. 1993).

[26] 139 Cong. Rec. S15762 (Nov. 16, 1993).

[27] *Id*; 139 Cong. Rec. S15765 (Nov. 16, 1993)(statement of Sen. Robb).

[28] 139 Cong. Rec. S15762 (Nov. 16, 1993).

[29] 139 Cong. Rec. S15764 (Nov. 16, 1993).

[30] 139 Cong. Rec. S15765 (Nov. 16, 1993).

[31] *Id*.

[32] Driver's Privacy Protection Act of 1993, H.R. 3365, 103rd Cong. (1st Sess. 1993).

[33] 139 Cong. Rec. E2747 (Nov. 3, 1993).

[34] 139 Cong. Rec. H2522 (Apr. 20, 1994).

[35] Abram Chayes, *The Role of the Judge in Public Law Litigation*, 89 Harv. L. Rev. 1281, 1283 (1976).

[36] Frederick Lodge, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 Fordham L. Rev. 611, 612 (1984).

[37] *The Right to Privacy*, 4 Harv. L. Rev. 193, 219 (1890) ("Even in the absence of special damages, substantial compensation could be allowed for injury to feelings as in the action of slander and libel.").

[38] *See, e.g.*, Mark E. Budnitz, *Privacy Protection For Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C. L. Rev. 847, 883 (1998).

[39] Jay Weiser, *Measure of Damages for Violation of Property Rules: Breach of Confidentiality*, 9 U. Chi. L. Sch. Roundtable 75, 100 (2002).

[40] Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1232-3 (April 2003).

[41] *Id*. at Fn. 27.

[42] Jonathan L. Entin, *The Right to Privacy One Hundred Years Later: Privacy Rights and Remedies*, 41 Case W. Res. L. Rev. 689, 693 (1991).

[43] Frank P. Anderano, *The Evolution of Federal Computer Crime Policy*, 27 Am. J. Crim. L. 81, 98 (1999).
