12-0661-cv

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

Erik H. Gordon,

Plaintiff-Appellant,

v.

JOHN DOES 1 through 10,

Defendants,

ARON LEIFER, aka JACK LOREN, BODYGUARDS.COM,

Defendant-Cross-Defendant-Cross-Claimant,

SOFTECH INTERNATIONAL, INC., REID RODRIGUEZ, ARCANUM INVESTIGATORS, INC., DAN COHN, aka DAN COHN,

Defendants-Cross-Claimants-Cross-Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER IN SUPPORT OF APPELLANTS AND URGING REVERSAL

Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140

June 15, 2012

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c) for Case No. 12-661

Amicus curiae Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTEREST OF AMICUS CURIAE

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values.[1]

EPIC routinely participates as *amicus curiae* before the United States Supreme Court, federal circuit courts, and state appellate courts in cases concerning privacy issues, new technologies, and constitutional interests, such as: *FAA v. Cooper*, 132 S. Ct. 1441 (2012); *United States v. Jones*, 132 S. Ct. 945 (2012); *First Am. Fin. Corp. v. Edwards*, 610 F.3d 514 (9th Cir. 2010), *cert. granted* 131 S. Ct. 3022 (2011); *Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653 (2011); *NASA V. Nelson.*, 131 S. Ct. 746 (2011); *Doe v. Reed*, 130 S. Ct. 2811 (2010); *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619 (2010); *Flores-Figueroa v. United States*, 556 U.S. 646 (2009); *Hiibel v. Sixth Judicial Circuit of Nev.*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Reno v. Condon*, 528 U.S. 141 (2000); *SEC v. Rajaratnam*, 622 F.3d 159 (2d Cir. 2010); *In re Google Inc. St. View*

[1] Appellant Gordon consents to the filing of this brief. Appellees Softech et al. do not consent to the filing of this brief. EPIC has submitted a motion for leave to file contemporaneous with this brief pursuant to Fed. R. App. P. 29(b). In accordance with Rule 29, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

Commn'cs, 794 F. Supp. 2d 1067 (N.D. Cal. 2011), *appeal docketed*, *Ben Joffe v. Google*, No. 11-17483 (9th Cir. Oct. 17, 2011); *Harris v. Blockbuster Inc.*, 622 F. Supp. 2d 396 (N.D. Tex. 2009), *appeal docketed*, No. 09-10420 (5th Cir. Apr. 29, 2009).

EPIC has a particular interest in ensuring the effective enforcement of federal statutes that seek to protect the privacy of personal information. The core purpose of the Driver's Privacy Protection Act is to ensure that the personal information obtained by state agencies for the issuance of licenses is used only for the permissible purposes set out in statute. The Act should be construed to impose strict liability on those companies that resell this information when it is subsequenly used for an impermissible purpose. It is both fair and economically efficient to place the burden on the reseller for the subsequent impermissible use of detailed, personal information that is protected under a federal privacy law and made available by the reseller.

SUMMARY OF THE ARGUMENT

There are over 210 million licensed drivers in the United States, and over 240 million licensed vehicles. Each vehicle displays a license plate number that can be uniquely linked to detailed personal information about a registered driver, including home address, height, weight, race, and organ donation status. The government requires individuals to provide this information as a condition of

obtaining a license to drive a vehicle on the public roadways. This sensitive personal information has been misused with harmful, and sometimes deadly, consequences. Individuals whose personal information has been disclosed by state departments of motor vehicles have been stalked and even killed by those who wrongfully obtained this information.

To protect the privacy and safety of licensed drivers and to limit misuse of the information contained in these government record systems, Congress enacted the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725. The Act imposes strict rules for collecting the personal information in driver records, and provides for liability in cases where a person improperly collects, discloses, uses, or sells such records. There are some companies that collect information under the Act for investigatory purposes, such as the settlement of insurance claims, but this narrow permissible purpose does not constitute an open-ended opportunity to routinely resell the personal information obtained from the state records system. 18 U.S.C. § 2721(c).

To ensure that this exception is not abused and that the privacy of driver records is adequately protected under the Act, it is necessary to impose strict liability on resellers when the records they sell are subsequently used for an impermissible purpose. As the reseller is in the best position to determine whether the subsequent use of the data would be permissible under the Act, it is the reseller

that must bear the burden of ensuring that an impermissible use does not occur. The state agency ceases to be the custodian of the data once it is obtained by the reseller; the reseller must therefore assume the responsibility and the liability for the subsequent use of the data resulting from its intentional resale.

ARGUMENT

The Driver's Privacy Protection Act of 1994 (the "DPPA"), 18 U.S.C. §§ 2721-2725, was enacted to prevent unauthorized access to "an individual's identity and address on the basis of that individual's license plates." 139 Cong. Rec. 29,468 (1993) (statement of Sen. Warner). The Act's civil action section, 18 U.S.C. § 2724, provides that "[a] person who knowingly obtains, discloses, or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court." *Id*. Thus, the Act holds third parties liable for any impermissible use or disclosure of a driver record. Courts have made clear that there is no requirement that a defendant know or intend that an impermissible use will occur. *See, Pinchler v. UNITE*, 228 F.R.D. 230, 242 (E.D. Pa. 2005), *aff'd*, 542 F.3d 380 (3d Cir. 2008); *Best v. Berard*, ___ F. Supp. 2d ____, 2011 WL 5554021 at *8 (N.D. Ill. 2011); *Rios v. Direct Mail Express, Inc.*, 435 F. Supp. 2d 1199, 1204-05 (S.D. Fla. 2006); *Cowan v. Codelia*, No. 98-5548, 1999 WL 1029729 at *8 (S.D.N.Y. Nov. 10, 1999).

The Act only authorizes resale of driver records "for a use permitted under subsection (b)." 18 U.S.C. § 2721(c). Congress recognized the importance of regulating this commercial activity, where individuals are required to provide personal information to a state agency to obtain a license and this information is then made available for other purposes. Congress established these restrictions because of the danger that unfettered access to sensitive driver records poses for the millions of registered drivers in each state, which is similar to that posed by the sale of potentially unsafe and hazardous products. *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 Cal. L. Rev. 1805, 1845 (2010).

Accordingly, resellers are strictly liable whenever they sell information from a record that is used for an improper purpose. This strict liability for resellers is necessary to ensure that the purposes of the Act are fulfilled. Regarding the subsequent disclosure of information obtained under the Act, the legislative history of the Act makes clear that it incorporated "the intentions of the 1974 Privacy Act …. [And also] include[d] the recommendations of the 1977 Privacy Protection Study Commission [("PPSC")] report." *Id*. The goal was to prohibit disclosure of "records" collected and maintained by a Government agency, except under permissible circumstances. *See* 5 U.S.C. § 552a(b). The PPSC report recommended that third party record holders be held to the "same standard" as the Government in order to ensure compliance with the important statutory protections. Personal

Privacy in an Information Society: The Report of the Privacy Protection Study Commission ch. 13 (July 1977). The Act incorporated these recommendations, and thus it imposes civil liability on a company who resells information from a government DMV record, except in the narrow instance where that record is used for an enumerated permissible purpose.

I. Strict Liability for the Improper Sale of Driver Records is Necessary to Satisfy the Statutory Purpose of the DPPA

In *Reno v. Condon*, 528 U.S. 141 (2000), the Supreme Court made clear that that the DPPA ("the Act") permissibly "regulates the universe of entities that participate as suppliers to the market for motor vehicle information … private resellers or redisclosers of that information in commerce." *Id.* at 151. The Act was passed in response to the practice of selling the information that the Departments of Motor Vehicles ("DMVs") required individuals to provide as a condition of obtaining a drivers license. This practice made sensitive personal information available to strangers for purposes unrelated to the issuance of licenses. Congress had good reason to believe that the unregulated sale of motor vehicle records presented a particular threat to privacy and personal safety.

In New York, for example, motor vehicle records contain a wealth of personal information, including name, date of birth, mailing address, driver license class, endorsements, restrictions, expiration date of the driver license, suspensions or revocations of the driver license, accidents, moving violation convictions,

vehicle information, and title and lien information. *See* New York State Dept. of Motor Vehicles, *What Information Appears on DMV Records?*[2] Individuals who wish to drive must surrender this information, which is then sold by the DMV and resold by companies such as Docusearch.[3]

Furthermore, the sale of these records resulted in a wide range of abuses across the country, with disastrous consequences. *See* 140 Cong. Rec. H2522 (daily ed. Apr. 20, 1994) (statement of Rep. Moran) (describing the case of Rebecca Schaeffer, who was "gunned down at her Los Angeles apartment, by a man who had—through a private investigator—obtained her home address from the California DMV."). Resellers, such as Docusearch, similarly disclose sensitive driver records for a commercial purpose, and should be liable under the Act for subsequent misuse and harm caused by their disclosure.

---

[2] http://www.dmv.ny.gov/abstract.htm#WHAT (last visited June 14, 2012).

[3] Docusearch is an internet-based investigation and information service operated by Arcanum Investigations, Inc. Docusearch represents itself as "America's premier provider of on-line investigative solutions" and emphasizes the ease with which buyers can access personal information:

> Requesting investigative services has never been easier than using our web site. Our user-friendly interface will prompt you for all the necessary data. Once an assignment is complete, you will be notified by email that the results have been posted in a secure, password protected client area. It doesn't get any easier than that!

About Us, Docusearch.com, http://www.docusearch.com/about.html (last visited June 15, 2012).

Strict liability for resellers is necessary to ensure fairness to individuals, who are subjected to mandatory Government record-keeping requirements and the efficiency of the market for personal information. Strict liability ensures that individuals who are harmed by the improper sale of their personal information can assert their rights, without imposing the heavy burden of establishing a tort-based negligence claim. Strict liabilty is also necessary to ensure that commercial vendors of a dangerous product (here sensitive personal information) internalize the cost of harms caused by that product's use.

Furthermore, resellers clearly serve a "gatekeeper" function in the market for personal information because they review buyer requests and ensure compliance with DPPA restrictions. The possibility of liability gives resellers "incentive to adopt appropriate policies and procedures to prevent the misuse of motor vehicle records, thereby furthering the DPPA's goals of protecting individuals' personal information." *Margan v. Niles*, 250 F. Supp. 2d 63, 75 (N.D.N.Y. 2003). Here the resellers' only precaution was to require customers to check a "box" from a list of permissible uses. This minimal level of effort is not sufficient to meaningfully protect driver records, and should not relieve resellers of liability under the Act. Strict liability is particularly important where, as here, resellers "have relatively easy, free, and unfettered access to motor vehicle records, which … can lead to unchecked abuse." *Id.* at 74.

Finally, resellers must be held strictly liable to provide a meaningful deterrent for impermissible uses of driver records. Buyers who misuse driver records provide false names or contact information to resellers, especially if they intend to cause harm, and will not be deterred by strict liability in the same way as resellers active in the market for personal data. The disclosure of driver records, absent statutory protections and accountability, poses a real and unavoidable threat to most Americans, who are required by law to register with their state DMVs and submit personal information for these records.

II. Resellers of DMV Records Should Be Strictly Liable for the Subsequent Impermissible Use of Personal Data They Have Sold

The DPPA was enacted to provide statutory protection for the sensitive personal information contained in driver records. Resellers and users of these driver records are liable whenever they do not satisfy the "permissible purpose" requirements of Section 2721(b).[4] This strict liability is necessary for several reasons. First, strict liability is necessary to avoid the evidentiary burden imposed on injured parties by traditional negligence law. Second, strict liability ensures that a reseller limits the sale of sensitive data and take precautions to avoid misuse.

[4] The "Insurance - Other" designation that the buyer selected when purchasing the motor vehicle information from Docusearch apparently corresponds to 18 U.S.C. 2721(b)(6). But that provision only allows the use of personal information in state motor vehicle records "by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, antifraud activities, rating or underwriting," which the buyer clearly was not.

Strict liability has long been recognized as solving enforcement problems that commonly occur in a commercial context, where harms resulting from negligence can be difficult to prove. Mark Geistfeld, *Negligence, Compensation, and the Coherence of Tort Law*, 91 Geo. L. J. 585, 619 (2003).[5] Courts have recognized enforcement as one of the "principal purposes behind" strict liability in the commercial context. *Barker v. Lull Eng'g Co.*, 573 P.2d 443, 455 (Cal. 1978) ("to relieve an injured plaintiff of many of the onerous evidentiary burdens inherent in a negligence cause of action."). This rationale is equally applicable in this context, where an individual harmed by a stalker or harrasser would have to shoulder the difficult burden of discovering and rebutting the resellers' arguments that they were not aware of or involved in the alleged impermissible use. Stalkers can attempt to escape liability by concealing their identity. In *Remsburg v. Docusearch, Inc.*, for example, the victim's work address was obtained through "pretexting," where a subcontractor "lied about who she was and the purpose of her call in order to convince [the victim] to reveal her employment information." 816 A.2d 1001, 1006 (N.H. 2008). In the instant case, Aron Leifer, Docusearch's "customer," created an account using the alias "Jack Loren," claimed to work for

[5] *See also* Richard A. Epstein, *Causation – In Context: An Afterword*, 63 Chi.-Kent L. Rev. 653, 663 n.25 (1987) ("The ground on which a rule of strict obligation has been maintained and consolidated by modern authorities is the magnitude of danger, coupled with the difficulty of proving negligence as the specific cause, in the particular event of the danger having ripened into actual harm.").

an imaginary company called Bodyguards.com, and listed a fake address. The deception employed by buyers, such as Leifer, from commercial resellers of information makes it particularly difficult for victims to enforce their privacy rights. It is the reseller of the data, not the victim, that is best positioned to detect and prevent this fraudulent conduct.

Strict liability also helps ensure that the reseller will limit subsequent disclosure to those that are permitted under the Act. Under a traditional economic analysis of law, negligence liability will create an inefficient outcome where a seller's product causes harm to a stranger. *See* Steven Shavell, *Strict Liability Versus Negligence*, 9 J. Legal Stud. 1, 3 (1980). The seller will not limit its sale of personal information under a negligence standard because the court will only review the level of care exercised in creating and marketing that product. *Id.* Thus, as long as a reseller observes the level of care required by the negligence standard, there is no limit to the amount of times it can sell personal information. The purpose of the DPPA, however, was to *limit* the sale and subsequent use of driver record information to those specifically set out in Section 2721(b). Where the use is not permissible, it is a *per se* violation of the Act,

Some courts have already imposed on resellers for the impermissible disclosure or resale of personal information in the tort privacy context. In *Remsburg*, the Supreme Court of New Hampshire held that tort law imposes a duty

on resellers to exercise reasonable care when disclosing personal information to third parties. 816 A.2d at 1008. This duty exists because the resale of personal information creates "an especial temptation and opportunity for criminal misconduct brought about by the defendant." *Id.* at 1007 (citation and quotation omitted). In particular, resale presents the risks of "stalking and identity theft." *Id.* at 1008. By imposing liability on resellers, the court in *Remsburg* sought to provide some incentive for resellers to prevent harmful disclosures.

The United States Court for the District of Columbia Circuit considered a similar issue in *Schuchart v. La Tabema Del Albardero, Inc.*, 365 F.3d 33 (D.C. Cir. 2004), where customers sued a restaurant for disclosing personal financial information to their employer. The plaintiffs in *Schuchart* sought relief for intrusion upon seclusion, a privacy tort. *Id*. at 37. While the court could not conclusively answer the question of whether state tort law imposes liability on a third party for disclosure of personal information "limited to use for only certain purposes," the court noted that "the degree of protection afforded privacy interests … is a matter of public importance." *Id*. *Cf Berry v. Watchtower Bible & Tract Soc. of N.Y., Inc.,* 879 A.2d 1124, 1128-29 (N.H. 2005) (recognizing common law duty where defendant's actions "create an especial temptation and opportunity for criminal misconduct.").

Tort law may well establish a duty to safeguard personal information from misuse by others. But where Congress has passed a law to regulate the collection and use of personal information, there is no question that such a duty exists. Congress enacted the Drivers Privacy Protection Act specifically to prevent the misuse of information obtained by the state DMVs. Unlike the tort law at issue in *Schuchart*, the Act clearly provides for liability where a company sells information from a driver record that is subsequently used for an impermissible purpose. 18 U.S.C. § 2721(b).

III. Strict Liability is Necessary to Ensure That Resellers Take Precautions to Avoid Impermissible Uses

The purpose of the Act is to prevent and limit misuse of driver records maintained by state departments of motor vehicles. To this end, the Act prohibits intentional use or disclosure of records, except for permitted uses. Authorized resellers can only disclose information from these records for a permissible use. Without this limitation on resale, the protections of the Act could be circumvented by third parties who obtain all driver records through resellers without limitations or liability. By imposing strict liability on resellers, the Act imposes an incentive on those companies to implement precautionary procedures to prevent abuse of driver records. Absent liability, resellers will have no reason to verify that buyers use their real identities or have adequate documentation of their permissible purpose.

Strict liability is necessary to ensure that the Act's prohibition on disclosure of personal information absent a permissible use. 18 U.S.C. § 2721. The provision allows recovery of actual, punitive, and liquidated damages ($2,500) in addition to reasonable attorneys fees and other equitable relief. *Id*.[6] The purpose of this provision is twofold: to compensate individuals for the improper disclosure of their personal information, and to ensure compliance with the statutory protections.

Liability typically serves this dual purpose in civil law. In law and economic literature, liability has been analyzed both in the context of accidents[7] and in the context of sanctions.[8] The Act liability mechanism can be justified similarly to

[6] The Act's civil damages provision is typical for a statutory privacy law. Such laws routinely establish liability for breaches or misuses of personal information. The Video Privacy Protection Act of 1988, 18 U.S.C. § 2710, the Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, the Cable Communications Policy Act of 1984, 47 U.S.C. § 521 et seq., the Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227, the Right to Financial Privacy Act of 1974, 12 U.S.C. § 3401, and the Privacy Act of 1974, 5 U.S.C. § 552a, all provide for the recovery of civil damages (including liquidated damages) in case of a privacy violation.

[7] *See* Steven Shavell, *Liability for Accidents* (Handbook of Law and Economics, Vol. 1, A. Mitchell Polinsky and Steven Shavell, eds., Elsevier, 2007, 139-182); Richard Posner, *Economic Analysis of Law* (5th ed. 1998); Guido Calabresi & A.D. Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harv. L. Rev. 1089 (1972); Guido Calabresi, *Concerning Cause and the Law of Torts* (1970).

[8] *See* Steven Shavell, *The Theory of Public Enforcement of Law* 407 (Handbook of Law and Economics, Vol. 1, A. Mitchell Polinsky and Steven Shavell, eds., Elsevier, 2007, 403-454).

other "accident" liability rules[9] because the party responsible for the misuse of records acts without the knowledge or consent of the individual whose record is disclosed.[10] *See* Shavell, *supra* note 7, at 143 (describing conditions for the economic analysis of liability incentives).

There has long been a consensus among legal scholars that such liability is necessary to protect privacy rights. As Warren and Brandeis explained in the famous law review article establishing the right to privacy, privacy violations give rise to liability even where "[p]ersonal ill-will is not an ingredient."

> The invasion of the privacy that is to be protected is equally complete and equally injurious, whether the motives by which the speaker or writer was actuated are, taken by themselves, culpable or not …. Viewed as a wrong to the individual, this rule is the same pervading the whole law of torts, by which one is held responsible for his intentional acts, even though they are committed with no sinister intent … it is the same principle adopted in a large category of statutory offenses.

Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 218-19 (1890).

---

[9] Alternatively, the civil liability provisions in the Act can be viewed as a kind of monetary sanction, imposed by the Government through direct or private action. *See* Shavell, *supra* note 7, at 407. Though, even if interpreted as a sanction, the ultimate goal of the provision is still to deter harmful behavior (improper disclosure and use of driver records). The damages award should be interpreted in such a way as to meaningfully limit misuse of personal information. *Id.* at 435.

[10] An accident is considered "unilateral" when "only injurers can influence risks." Shavell, *supra*, note 7 at 143. It is easier to measure the predicted effect of liability in case of a unilateral accident because the liable party's actions alone contribute to the harmful outcome. *Id.*

As Professor Alessandro Acquisti has more recently described, rules that impose liability on a party responsible for a breach or misuse of personal information ("ex post liability rules") serve "as a deterrent for firms by raising their expected costs of engaging in some harmful activity and compensating injured parties for their loss." Alessandro Acquisti & Sasha Romanosky, *Privacy Costs and Personal Data Protection: Economic and Legal Perspectives*, 24 Berkeley Tech. L. J. 1061, 1072 (2009). In this way, privacy laws provide "a legal device that enables victims to sue for damages, forcing firms to internalize part of the harm they cause." *Id.* at 1068.

Imposing liability on resellers promotes economic efficiency. The relationship between individuals and resellers, such as Docusearch, is plagued by information asymmetries. *See Understanding Consumer Attitudes About Privacy: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the House Comm. on Energy and Commerce* (Oct. 13, 2011) (testimony of Prof. Alessandro Acquisti).[11] Compared to individuals, who have no control over their driver records, resellers are in a better position to control the subsequent use of the personal data in their possession according to DPPA restrictions. Because resellers control the flow of this information, they are the "least cost avoider"—the party

[11] *Available at* http://republicans.energycommerce.house.gov/Media/file/Hearings/CMT/101311/Acquisti.pdf.

who can more efficiently take preventative measures to avoid misuse. *See* Guido Calabresi, *The Cost of Accidents: A Legal and Economic Analysis* 136-38 (1970) (applying the least cost avoider to a typical car accident scenario). Liability rules that hold a least cost avoider responsible allocate rights and responsibilities such that individual data is protected and statutory violations are avoided.

State departments of motor vehicles recognize the threat of downstream resale and misuse of sensitive driver records. The New York DMV, for example, requires that any person applying for records certify their DPPA permissible use, and agree to indemnify and otherwise defend damages for "negligent, improper or unauthorized use or dissemination of the information provided by the DMV." N.Y. State DMV, *Instructions for Requesting DMV Record Information Using Form MV-15* (Dec. 2010).[12] Therefore "negligent disclosure" is clearly contemplated by any person (including a reseller) who requests records from NY and other state DMVs. Given the legally acknowledged sensitive nature of driver records, the requisite level of care in "disseminating" personal information should be higher. As Professor Citron has explained, data breaches and other inadvertant disclosures of personal information should be analyzed under the same strict liability standards as those governing hazardous materials. *See* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 Cal. L. Rev. 1805, 1844-48 (2010). Congress recognized in the

[12] *Available at* http://www.dmv.ny.gov/forms/mv15.pdf.

DPPA that the personal information contained in driver records is equally hazardous because it can be used to cause great harm, and resellers should be strictly liable for that harm as Professor Citron suggests.

Even Docusearch acknowledges the signficant risk in the resale of drivers records information and the fiduciary obligation to safeguard this data. According to Docusearch website,[13] most online companies offering "license plate lookups" "are scams!" But licensed private investigators, such as Docusearch, "are controlled by state regulatory agencies and are held to a high standard." WebScams.org, *Who Offers License Plate Lookups?* (June 8, 2012).[14] The site goes on to explain that websites offering "instant results" to reverse license plate requests are not legitimate because "only licensed investigators have access" and are "computer connected to the state DMV's [sic] in 26 states, and growing." WebScams.org, *Reverse Plate "Instant Results" Claims Debunked* (June 8, 2012).[15]

Holding resellers strictly liable under the DPPA for impermissible uses of the personal information they sell will ensure that reseller internalize the costs of privacy violations. Strict liability also gives a measure of control back to the

[13] *See* WebScams.org, *Disclosure Statement* (June 8, 2012), http://www.webscams.org/disclosure-statement/.
[14] http://www.webscams.org/who-offers-license-plate-lookups/.
[15] http://www.webscams.org/instant-results-claims-debunked/.

individuals whose information is being exploited and ensure that privacy harms are adequately compensated.

Resellers of personal information obtained from state record systems, subject to federal privacy law should not obtain the commercial beneft of selling someone else's personal information without also bearing the burden for the impermissible use of the product they are selling.

CONCLUSION

Amicus Curiae Electronic Privacy Information Center respectfully requests this Court to grant Appellant's motion to reverse the decision of the lower court.

Respectfully submitted,

/s/
Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140

June 15, 2012

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of 7,000 words of Fed. R. App. P. 29(d) and Fed. R. App. P. 32(B)(i). This brief contains 4,516 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word Mac in 14 point Times New Roman style.

Dated: June 15, 2012

___*/s/*_____

Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF SERVICE

I hereby certify that on this 15th day of June, 2012, the foregoing Brief of *Amicus Curiae* was electronically filed with the Clerk of the Court, and thereby served upon counsel for the parties *via* electronic delivery.

Dated: June 15, 2012

___/s/_____

Marc Rotenberg
Counsel of Record
Alan Butler
David Jacobs
Electronic Privacy
Information Center (EPIC)
1718 Connecticut Ave. NW,
Suite 200
Washington, DC 20009
(202) 483-1140