Case No. 14-1754

IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

Johanna Beth McDonough,

Plaintiff-Appellant,

v.

Anoka County et al.,

Respondents-Appellees.

On Appeal from the United States District Court
For the Northern District of Minnesota

BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLANT

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

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1 and 29(c), *Amicus Curiae* Electronic Privacy Information Center ("EPIC") is a District of Columbia corporation with no parent corporation. No publicly held company owns 10 percent or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF AMICUS

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

The Driver's Privacy Protect Act of 1994, ("DPPA") 18 U.S.C. §§ 2721–2725 (2012), was enacted to protect individuals from unauthorized disclosures of personal information collected by state DMVs. The Act prohibits the disclosure, except in narrow circumstances, of sensitive personal information that individuals are required to provide to obtain identification documents, drivers licenses, and automobile titles. Congress recognized that the improper release of this information creates a significant risk of physical and financial harm.

EPIC has filed several *amicus* briefs, urging federal courts to uphold the intent of the Act. *See, e.g., Maracich v. Spears*, 133 S. Ct. 2191

[1] Appellant McDonough consents to the filing of this brief. Appellees Anoka County 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.

(2013); *Reno v. Condon*, 528 U.S. 141 (2000); *Gordon v. Softech Int'l Inc.*, 726 F.3d 42 (2d Cir. 2013); *Kehoe v. Fidelity Fed. Bank & Trust*, 421 F.3d 1209 (11th Cir. 2005).

SUMMARY OF THE ARGUMENT

The Driver's Privacy Protection Act established the critical safeguard for sensitive personal information collected and held by state Departments of Motor Vehicles. Congress passed the DPPA after it determined that the improper disclosure of an individual's driver records could lead to identity theft, stalking, and even homicide. But the harms stemming from compromised personal information are not always apparent, and in many cases are not discoverable for years. Because drivers have very little knowledge about how the personal information they have provided to the DMVs will be used by others, it is necessary, to fulfill the purposes of the Act, to delay the accrual of time under the statute of limitations until the victim knows or could reasonably discover that their data has been impermissibly used.

ARGUMENT

The Minnesota Department of Public Safety ("DPS") makes drivers' motor vehicle records accessible to law enforcement officers through its electronic Driver and Vehicle Services ("DVS") database. Plaintiff Johanna McDonough requested an audit[2] of her personal DVS record from DPS in 2013. This "audit showed that the record has been accessed hundreds of times from facilities maintained by defendant counties and cities." *McDonough v. Al's Auto Sales, Inc.*, ___F. Supp. 2d___, 2014 WL 683998, at *1 (D. Minn. Feb. 21, 2014). In response, McDonough filed suit against various counties and cities, and the current and former commissioners of DPS, alleging violations of her rights under the

[2] Under the Minnesota Government Data Practices Act, any individual can access the "audit trail" associated with their driver's license records, and thereby learn when and how their records were accessed. *See* Minn. Stat. 13:03 (2013) ("Upon request to a responsible authority or designee, a person shall be permitted to inspect and copy public government data at reasonable times and places, and upon request, shall be informed of the data's meaning.") *See also* Steve Drazkowski, *How to Obtain Your Drivers License Access Audit Trail Data* (Sept. 14, 2013) (describing how Minnesota drivers can access their data through the Driver Vehicle Services [DVS] and the Bureau of Criminal Apprehension [BCA] systems, in order to obtain a complete audit trail history), *available at* http://www.draz.com/2013/09/how-to-obtain-your-drivers-license-access-audit-trail-data/.

DPPA, her civil rights under 42 U.S.C. § 1983 (2012), and other constitutional common law privacy rights.

The district court ruled that DPPA claims related to records accessed prior to July 12, 2009 were time-barred because they were outside the applicable statute of limitations. *McDonough,* 2014 WL 683998, at *2. The district court then dismissed the timely DPPA claims against the commissioners, cities, and counties for failure to state a claim under the pleading standards set out by the Supreme Court in *Bell Atl. Corp. v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009). *McDonough*, 2014 WL 683998 at *2–4.

The DPPA has no express statute of limitations, and therefore courts have applied the general four-year statute of limitations for federal statutory claims. *See* 28 U.S.C. § 1658(a) (2012) ("Except as otherwise provided by law, a civil action arising under an Act of Congress . . . may not be commenced later than 4 years after the cause of action accrues"). However, courts have disagreed on when a DPPA cause of action accrues and when the four-year time period begins to run.

Courts have established two different approaches to calculating the accrual for the statute of limitations. The first approach is known as the

"occurrence rule," where the claim accrues "when the plaintiff has 'a complete and present cause of action.'" *Wallace v. Kato*, 549 U.S. 384, 388 (2007) (citing *Bay Area Laundry & Dry Cleaning Pension Trust Fund v. Ferbar Corp. of Cal.*, 522 U.S. 192, 201 (1997)). The second approach is known as the "discovery rule," where accrual is delayed "until the plaintiff has 'discovered'" the offense. *Merck & Co. v. Reynolds*, 559 U.S. 633, 644 (2010). The Supreme Court has explained that the word discovery in this context "refers not only to the plaintiff's *actual* discovery of certain facts, but also to the facts that a reasonably diligent plaintiff would have discovered." *Id.* (emphasis in original). The discovery rule originated first in fraud cases because the Court recognized "something different was needed" where "a defendant's deceptive conduct may prevent a plaintiff from even *knowing* that he or she has been defrauded." *Id.* (emphasis in original).

Since the Court first established the discovery rule in the fraud context, it has extended the application beyond fraud cases by statute and judicial implication. The Court has extended the discovery rule to claims for latent disease and medical malpractice "where the cry for [such a] rule is loudest." *Rotella v. Wood*, 528 U.S. 548, 555 (2000).

When the Court has considered extending the rule in the past it has looked for "textual, historical, or equitable reasons to graft a discovery rule" onto a statute of limitations. *Gabelli v. SEC*, 133 S. Ct. 1216, 1224 (2013).

I. The Discovery Rule Should Apply to DPPA Claims Because Historical and Equitable Considerations Favor Delaying Accrual of the Statute of Limitations

A. The DPPA Was Enacted to Protect Personal Information, the Improper Disclosure of Which Would Be Difficult to Detect

Congress enacted the DPPA in 1994 to provide protection for the sensitive information collected by State Departments of Motor Vehicles ("DMVs").[3] Congress also emphasized that "[r]andom access to personal information contained in DMV files poses a threat to every licensed driver in the Nation. In my own State of Virginia, over 127,815 requests are made every year for personal information contained in motor vehicle files. In Virginia, like most other States, licensees are not notified that their personal information has been accessed." 139 Cong. Rec. E2747 (daily ed. Nov. 3, 1993) (statement of Rep. James Moran, a sponsor of the Act). Another sponsor of the Act noted that "[t]here is a war in this

[3] *See* EPIC, *The Driver's Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record* (2013), *available at* http://epic.org/privacy/drivers/.

country to fight for privacy. People are now fighting, and this [Act] is coming to their assistance to provide the privacy, which I and many others thought existed." 139 Cong. Rec. S15,764 (daily ed. Nov. 16, 1993) (statement of Sen. John Warner).

The DPPA provides that "[i]t shall be unlawful for any person knowingly to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." 18 U.S.C. § 2722. The DPPA also provides individuals with a cause of action against any "person who knowingly obtains, discloses, or uses [their] personal information, from a motor vehicle record, for a purpose not permitted under" the Act. 18 U.S.C. § 2724(a).

The DPPA defines "personal information" as "an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information." 18 U.S.C. § 2725(3). The DPPA also provides additional protections for "highly restricted personal information," which includes "an individual's photograph or image, social security number, medical or disability information." 18 U.S.C. § 2725(4). The DPPA prohibits use or disclosure of this highly sensitive information,

except for four permissible uses. 18 U.S.C. § 2721(a)(2). However, there is no provision in the Act by which individuals are notified when their personal information is disclosed to others.

1. The DPPA Prohibits Use of Driver Data Except for Certain Permissible Uses

In enacting the DPPA, Congress intended to limit impermissible uses of the information, while still providing access to the public in certain narrow circumstances. As Congressman Jack Brooks (D-TX), explained at the time:

> There are key differences between DMV records and other public records. There was no evidence before the subcommittee that other public records are vulnerable to abuse in the same way that DMV records have been abused. Unlike with license plate numbers, people concerned about privacy can usually take reasonable steps to withhold their names and address from strangers, and thus limit their access to personally identifiable information contained in voter registration lists, court records, or land records.

140 Cong. Rec. 7926 (1994) (statement of Rep. Jack Brooks). The DPPA permits certain limited uses of driver information but prohibits all other uses in order to prevent abuse. However, the DPPA prohibition only applies to those who "knowingly disclose or otherwise make available" the protected personal information. 18 U.S.C. § 2721(a). Because of this carefully crafted compromise, application of the discovery rule is

appropriate for equitable reasons. Even when an individual knows that their driver's record has been accessed, they may not know or have reason to know that the record was impermissibly used.

Because of this balance, the individual cannot reasonably avail themselves of their DPPA rights until they become aware of the impermissible use. Individuals are not notified when their records are accessed and might not find out until much later that their records were accessed for an impermissible purpose. Rather than having the statute of limitations begin to run when the impermissible use occurs, before the individual knows or could reasonably know that their rights have been violated, it would be equitable to accrue the statute of limitations based on the individual's discovery of the violation. Application of the discovery rule is appropriate because of this delayed notification and difficulties in distinguishing between permissible and impermissible uses.

2. *The Amount of Information Collected by State DMVs is Extensive and Highly Useful for Identity Theft*

The Supreme Court recently determined that the disclosure of the "highly personal information" collected by state DMVs would be "so substantial an intrusion on privacy it must not be assumed, without

language more clear and explicit," from Congress. *Maracich v. Spears*, 133 S. Ct. 2191, 2202 (2013). As the Court has recognized, this protection is necessary because "[s]tate DMVs require drivers and automobile owners to provide personal information" including Social Security Numbers ("SSNs") and other sensitive data. *Reno v. Condon*, 528 U.S. 141, 143 (2000). As EPIC explained to the Court, "DMVs now collect a staggering amount of personal information including biometrics, birth certificates, and other sensitive identifying information." Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) and Twenty-Seven Technical Experts and Legal Scholars in Support of the Petitioner, *Maracich v. Spears*, 133 S. Ct. 2191 (Nov. 16, 2012) (No. 12-25).[4] Individuals are required to provide this information to obtain even a simple state identification document. The Court in *Maracich* found that the extraordinary amount of sensitive information collected by the DMVs required a narrow construction of the statutory exceptions, and a strong presumption of privacy protection. 133 S. Ct. at 2196.

[4] *Available at* http://epic.org/amicus/dppa/maracich/EPIC-Maracich-v-Spears-Amicus-Brief.pdf.

B. Harms Arising from the Disclosure of Personally Identifiable Information Are Latent and Not Immediately Discoverable

Because SSNs and other sensitive personal data, obtained by DMVs, are used in such a wide variety of contexts, it may be months or years before an individual becomes aware that their data has been misused or that their identity has been stolen. Special protections are necessary for driver records because of the increasing risk of identity theft. Like fraud or an undisclosed defect, identity theft might not become apparent to the victim for years after their driver records have been accessed. Because of the potential for long-term damage and the inherent difficulty for individuals in determining when DPPA information has been misused, it is essential to apply the discovery rule to the statute of limitations for DPPA claims.

Federal and state government agencies recognize that combating identity theft is a top priority nationwide. *See* The President's Identity Theft Task Force, *The President's Identity Theft Task Force Report* (Sept. 2008).[5] It is particularly important to protect driver records

[5] *Available at* http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf.

because the personal information collected by state DMVs is precisely the type of data that identity thieves target. *See* Mark E. Vogler, *RMV Document Theft Prompts Identity Fraud Concerns*, Gloucester Times, Apr. 6, 2012. In particular, "[SSNs], along with a name and birth date, are the three pieces of information most often sought by identity thieves." U.S. Gov't Accountability Office, GAO-05-1016T, *Federal and State Laws Restrict Use of SSNs, Yet Gaps Remain* 3 (2005).[6] Once an identity thief obtains this information, they can use it "as 'breeder' information to create additional false identification, such as driver's licenses." *Id*. State DMVs hold all three pieces of information that are most valued by identity thieves. The SSN is also often used by private entities to verify the identities of customers, *id.* at 11, making them a highly desirable piece of information for identity thieves to access and stockpile for future exploits.

Armed with sensitive personal data, identity thieves can cause substantial harm. They can "drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief might even file a

[6] *Available at* http://www.gao.gov/assets/120/112174.pdf.

tax return in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest." Fed. Trade Comm'n, *Taking Charge: What to Do if Your Identity Is Stolen* 3 (2013).[7] In 2012 alone, more than 12.6 million Americans were affected by identity theft and incurred costs of more than $21 billion. Kristen Finklea, Cong. Research Serv., R40599, *Identity Theft: Trends and Issues* 1 (2014).[8] An estimated 14 percent of individuals aged 16 or older (34.2 million people) will experience identity theft at some point during their lives. Bureau of Justice Statistics, U.S. Dep't of Justice, *Victims of Identity Theft, 2012* at 11 (Dec. 2013).[9]

Identity theft can occur any time thieves gain access to sensitive personal records like those stored by state DMVs. The threat of identity theft underlies much of modern privacy law, including the DPPA, and provides a clear historical basis to extend the discovery rule in this context. Identity theft has been the top complaint category to the Federal Trade Commission for the past fourteen years. *See* Fed. Trade Comm'n, *FTC Announces Top National Consumer Complaints for 2013:*

---

[7] *Available at* https://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf.
[8] *Available at* http://www.fas.org/sgp/crs/misc/R40599.pdf.
[9] *Available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

Commission's Annual Report Shows Identity Theft Continues to Top List of Complaints (2013);[10] Fed. Trade Comm'n, *FTC Releases Top 10 Complaint Categories for 2012: Identity Theft Tops List for 13th Consecutive Year in Report of National Consumer Complaints* (2012).[11]

1. Identity Theft Is Not Easily Detected

Identity theft, like financial fraud, is not an injury that is easily detected. Studies have found that 65 percent of victims are not even aware their identities have been stolen. U.S. Gov't Accountability Office, GAO-09-759T, *Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain* 8 (2009).[12] Furthermore, "most identity theft victims (91%) did not know anything about the identity of the offender." Bureau of Justice Statistics at 5. Indeed, many identity thieves take active steps to hide the theft from the victims in order to have more time to take advantage of the stolen identity. One report notes that "[b]eyond amassing charges on a victim's credit card, identity thieves may sometimes change the billing address

[10] *Available at* http://www.ftc.gov/news-events/press-releases/2014/02/ftc-announces-top-national-consumer-complaints-2013.
[11] *Available at* http://www.ftc.gov/news-events/press-releases/2013/02/ftc-releases-top-10-complaint-categories-2012.
[12] *Available at* http://gao.gov/assets/130/122769.pdf.

so that the victim will not receive the bills and see the fraudulent charges, allowing the thief more time to abuse the victim's identity and credit." Finklea at 19. Another report emphasizes that, "[i]dentity theft is a serious problem because . . . it can take a long period of time before a victim becomes aware that the crime has taken place." GAO-09-759T at 2. The consequences of identity theft (and delay in discovery) can be extremely severe, whereby "[s]ome individuals have lost job opportunities, been refused loans, or even been arrested for crimes they did not commit." *Id.*

Discovering that your identity has been stolen can take a great deal of time and the harm often remains undiscovered until long after actual fraud occurs. One California resident recently had someone apply for a "fraudulent duplicate California Driver's license" under her name and it took her nearly a year to discover her identity had been stolen. Identity Theft Resource Ctr., *ITRC Fact Sheet 113: Changing a Social Security Number.*[13] By the time she discovered the fraud, a warrant for her arrest had been out for six months, based on the actions of the identity thief. But even after she corrected the fraudulent license and mistaken

[13] *Available at* http://www.idtheftcenter.org/Fact-Sheets/fs-113.html (last accessed June 3, 2014).

warrant, it wasn't until she moved and "tried to change the utilities into [her] name," that she discovered the thief "had been using [her] SSN as well." *Id.*

This is even more of a pressing problem with the information stored in the DPPA databases. There is no reason for motor vehicle consumers to know when their data is being used in impermissible ways and they have no statutory mechanism to alert them to the misuse or abuse of their information, because "there is no 'early detection' system for criminal identity theft . . . most victims learn of the perils of criminal identity theft by indirect means. These include notice of citation(s) from the courts, collection agency calls, and notice of warrant(s) of arrest." Privacy Rights Clearinghouse, *Fact Sheet 17g: Criminal Identity Theft: What to do If it Happens to You* (May 2013).[14]

2. Combating Identity Theft Has Become a National Priority

State DMV records have been targeted numerous times over the past decade, which has increased the risk of driver identity theft. In one case, a criminal in Oregon obtained possession of a significant portion of the DMV database and used the information to commit identity theft.

[14] *Available at* https://www.privacyrights.org/criminal-identity-theft-what-to-do-if-it-happens-to-you (last accessed June 3, 2014).

Natalie Brand, *Police Say Convicted Felon Charged with 50 Counts of ID Theft*, Fox Oregon (Mar. 24, 2012). Recently in Massachusetts, "[t]wo masked men stole several bags containing various records that included registration transactions, duplicate titles, crash reports, citation payments" and other state DMV records. Mark E. Vogler, *RMV Document Theft Prompts Identity Fraud Concerns*, Gloucester Times, Apr. 6, 2012. A similar theft of computers containing sensitive driver information occurred at a Connecticut DMV. Gregory B. Hladky, *Three Computers Stolen from DMV Held Personal Info*, New Haven Register, Dec. 21, 2007. The Colorado state DMV put more than three million drivers at risk by sending "large batches of personal information over the Internet without encryption" and failing to "properly limit access to its database." Jessica Fender, *DMV Puts Coloradans at Risk of ID Theft*, Denver Post, July 9, 2008.[15] Even these unintentional acts can put personal information at risk.

State DMVs recognize that identity theft is a significant problem and they emphasize the need to protect personal information and limit the risks to individuals. The California Department of Motor Vehicles notes

[15] *Available at* http://www.denverpost.com/news/ci_9822063.

that "[i]dentity theft and identity fraud are two of the fastest growing crimes in the United States." Cal. Dep't of Motor Vehicles, *Identity Fraud* (Aug. 2013).[16] The California Attorney General echoes these concerns and provides a California Identity Theft Registry, to attempt to avoid the consequences of criminal identity theft. State of Cal. Dep't of Justice, Office of the Attorney Gen., *How to Use the California Identity Theft Registry—A Guide for Victims of "Criminal" Identity Theft* (2014).[17] Similarly, the state of Pennsylvania has developed an "Identity Theft Action Plan," which includes resources, stories from victims of identity theft, prevention tips, and other guidance.[18] The Pennsylvania Department of Transportation acknowledges that "while identity theft is a crime, the perpetrator is often difficult to track" and recommends quick action to resolve identity theft. Penn. Dep't of Transp., *Protecting Yourself from Identity Theft/Consumer Fraud* (2014).[19]

---

[16] *Available at* http://apps.dmv.ca.gov/pubs/brochures/fast_facts/ffdl25.pdf.
[17] *Available at* http://oag.ca.gov/idtheft/facts/how-to-registry#theft.
[18] *Available at* http://www.portal.state.pa.us/portal/server.pt/community/identity_theft/9199 (last accessed June 4, 2014).
[19] *Available at* http://www.dmv.state.pa.us/identity_theft/index.shtml.

The North Carolina Attorney General also provides an "ID Theft Victim Toolkit," and emphasizes that "[t]aking action quickly is key . . . Do not give in no matter how frustrated you are." N.C. Dep't of Justice, *Help for Victims – ID Theft Victim Toolkit*.[20] With regard to driver's license information specifically, the North Carolina Attorney General advises that the victim contact the North Carolina DMV and "ask that they place a notation on the comments section of your license file. If a drivers license has already been acquired by an ID thief, request that they investigate the matter." N.C. Dep't of Justice, *ID Theft Victim Toolkit* (2006).[21] The official North Carolina Identity Theft Affidavit contemplates that the victim of the fraud may not have any prior knowledge that fraud may have occurred. In "Part II—How the Fraud Occurred," question 16 provides a box to check to assert the following: "I do NOT know who used my information or identification documents to get money, credit, loans, goods, or services without my knowledge or authorization." *Id.* at 9. As this indicates, the North Carolina Attorney General envisions that victims may not know how their information

[20] *Available at* http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims/ID-Theft-Victim-Toolkit.aspx (last accessed June 4, 2014).
[21] *Available at* http://www.ncdoj.gov/getdoc/91578f0c-87b6-43a5-ba77-4d172854c56b/ID-Theft-Victim-Toolkit.aspx.

was released or who used that information and emphasizes the necessity of a quick response in order to prevent further damage.

Identity theft has also become an increasingly important priority for state and federal law enforcement agencies. The U.S. Department of Justice, expressing deep concern over the increase in identity theft, unveiled a national strategy to combat the problem in 2006. Office of Cmty. Oriented Policing Servs., U.S. Dep't of Justice, *A National Strategy to Combat Identity Theft* (May, 2006).[22] The DOJ worked with local and state law enforcement to develop recommendations and a national approach that could be carried out through partnerships at the local, state, and national level. The report noted that identity theft was a threat because it could involve connections to violent crime or terrorism and also emphasized that "it may be even more complex because there is dual victimization: an individual and a financial entity. Frequently, the crime may not be discovered until long after its commission." *Id.* at 2.

President Bush also signed an executive order, creating the President's Identity Theft Task Force, consisting of senior cabinet

[22] *Available at* http://www.cops.usdoj.gov/Publications/e03062303.pdf.

leaders and chaired by the Attorney General. Exec. Order No. 13,402, 3 C.F.R. 225 (2007). The Task Force submitted a Strategic Plan to improve the federal government's response to identity theft, which it submitted on April 11, 2007, and then released a follow-up report in September 2008 on steps to implement the strategic plan. The Task Force made 31 recommendations, the first of which was to "Decrease the Unnecessary Use of SSN's in the Public Sector." The President's Identity Theft Task Force, *The President's Identity Theft Task Force Report* 6 (Sept. 2008).[23] The Task Force recognized that "[t]he SSN is highly valuable for identity thieves because it is often a necessary (if not necessarily sufficient) item of information that a thief needs to open new accounts in the victim's name." *Id*. at 6. Recommendation 18 urged the development of a "Universal Identity Theft Report Form," emphasizing that it could "facilitate the creation and availability of police reports, which victims need to exercise many of their . . . rights, such as placing a 7-year fraud alert on their credit file." *Id*. at 31. Without police reports, many victims are unable to assert their federal

[23] *Available at* http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf

rights and prevent future identity theft. The federal government recognizes the need to develop more effective mechanisms for identity theft victims. However, these mechanisms are all predicated on the notion that the victim will be aware of and capable of demonstrating that identity theft has occurred. This requirement and the exceptionally sensitive nature of the personal information at risk argue for the application of the discovery rule, rather than the occurrence rule.

C. The DPPA Seeks to Prevent Lurking Privacy Harms Caused by the Improper Disclosure of Personal Information Held by State DMVs

The DPPA is designed to help protect personal information that could be harmful if disclosed and lead to consequences such as identity theft. While there are steps individuals can take in the aftermath of identity theft, they are unable to take these steps until they in fact know that their identity has been stolen. For example, an individual can establish a fraud alert on their credit report, but the consumer "must have evidence of attempts to open fraudulent accounts and an identity theft report (police report) to establish the seven-year alert." Privacy Rights Clearinghouse, *Fact Sheet 17a: Identity Theft: What to*

Do if it Happens to You (Feb. 2014).[24] Even fraud alerts might not be enough and "may not entirely prevent new fraudulent accounts from being opened by the imposter. Credit issuers do not always pay attention to fraud alerts, even though the law requires it." *Id.* That is why consumer protection organizations recommend that you check your credit reports again in a few months. *Id.* The burden is on the consumer to detect the fraud and to respond to it by taking aggressive actions.

The harm caused by identity theft is not purely economic or monetary. Although non-economic harm is far more difficult to calculate, the psychological harm attached to identity theft can often be even more damaging. When one individual's SSN was accidentally associated with that of "an accused murderer with several DUI arrests," the harms were both economic and stigmatic. *ITRC Fact Sheet 113*. The individual noted, "I was now this man's alias and my jobs (potential and existing) were ruined. This cascaded into a bad line of credit due to my inability to obtain regular employment and eventually my marriage failed." *Id.* His economic harms (inability to gain a job) eventually led to the non-economic harm of losing his marriage. Even when he changed

[24] *Available at* https://www.privacyrights.org/content/identity-theft-what-do-if-it-happens-you.

his SSN and received a new SSN from the Social Security Administration, his "credit records now appeared to have a fraudulent SSN and the alert could only be seen by the creditors." *Id.* Unable to convince others of his true identity he concluded, "My entire future is an unknown . . . my life is in shambles." *Id.* A Bureau of Justice and Statistics study noted that "36 [percent] of identity theft victims reported moderate or severe emotional distress as the result of the incident." Bureau of Justice Statistics, U.S. Dep't of Justice, *Victims of Identity Theft, 2012*, at 1 (Dec. 2013). However, the theft of personal information often was far more distressing, as 32 percent of "victims of personal information fraud reported they found the incident severely distressing, compared to 5 [percent] of credit card fraud victims." *Id.* at 9. The theft of personal information, which constitutes the core of identity and is the type of information protected by the DPPA, was six times more likely to be viewed by victims as severely distressing compared to credit card fraud.

The harm that can result from the disclosure of DPPA information is precisely the type of "self-concealing injury" that the discovery rule is designed to ameliorate. As Chief Justice Roberts recently stated:

> [T]he discovery rule exists in part to preserve the claims of victims who do not know they are injured and who reasonably do not inquire as to any injury. Usually when a private party is injured, he is immediately aware of that injury and put on notice that his time to sue is running. But when the injury is self-concealing, private parties may be unaware that they have been harmed. Most of us do not live in a state of constant investigation; absent any reason to think we have been injured, we do not typically spend our days looking for evidence that we were lied to or defrauded. And the law does not require that we do so.

Gabelli, 133 S. Ct. at 1222.

II. The Discovery Rule Should Apply to DPPA Claims Because Drivers Will Never Have Sufficient Information to Adjudicate Claims Prior to Learning That Their Records Have Been Accessed

The discovery rule properly applies to the DPPA statute of limitations because the equitable and economic interests underlying the statutory prohibition on the improper disclosure of personal information favor longer-term protections for drivers. The DPPA was intended to allocate the responsibilities for data protection to the entity in possession of the personal data. Drivers have little or no information about how state DMVs handle and share their private records, and the principle of least cost avoidance supports delaying the accrual of the DPPA statute of limitations until after a victim had reason to know that their records were improperly used or disclosed.

In the absence of privacy legislation, tort law governs privacy harms. Tort law imports a number of assumptions: that both parties can identify each other, that they can identify the harm that has occurred, and that they can evaluate the cost of the harm. *See* Ronald H. Coase, *The Problem of Social Cost,* 3 J. L. & Econ. 1 (Oct. 1960). Where parties do not have this knowledge because they cannot know it — that is, because of systemic information asymmetries — legislation and common law rules must allocate the cost of informational discrepancies. Richard A. Epstein, *The Social Consequences of Common Law Rules*, 95 Harv. L. Rev. 1717, 1723–40 (1982). This is often achieved by determining which party is the "least cost avoider," or the party in the best position to prevent or mitigate the harm. Then the law can intervene to require that party to bear the burden of preventing or mitigating the harm. William M. Landes & Richard A. Posner*, The Economic Structure of Tort Law* 85–88 (1987). In the case of the DPPA, the parties who lack symmetrical information are the drivers, on one hand, and the DMVs that maintain the drivers' records, on the other. Since the DMVs will always be the least cost avoiders of privacy harms,

the DPPA must be construed to favor a limitations rule that allows the drivers extended access to redress.

Courts face a choice between accrual and discovery rules because the theory underlying statutes of limitations is bifurcated into opposing rationales. Both rationales weigh the courts' competing desires for perfect information and efficient resolution of claims. Eli J. Richardson, *Eliminating the Limitations of Limitations Law*, 29 Ariz. St. L.J. 1015, 1016 (1997) ("Limitations law ultimately aims at reconciling the delicate balance between plaintiffs' and society's interest in the pursuit of meritorious claims on the one hand, and defendants' and society's interest in avoiding the burdens of old claims on the other hand.") When courts must choose which rule to apply, they will frequently look to congressional intent and common law to find the core principle the law is meant to codify. The Harvard Law Review Ass'n, *Developments in the Law Statutes of Limitations*, 63 Harv. L. Rev. 1177, 1192 (1950). *See also United States v. Brockamp,* 519 U.S. 347 (1997) ("Is there good reason to believe that Congress did *not* want the equitable tolling doctrine to apply in a suit against the Government?") Where the purpose of a law is best substantiated by efficient resolution, courts will

choose the accrual rule; where the purpose of the law is defeated by an information asymmetry, courts will choose the discovery rule.

The standard accrual rule was traditionally favored where the resuscitation of old claims threatened the efficient adjudication of claims and normal functioning of the court system. Tyler T. Ochoa & Andrew J. Wistrich, *The Puzzling Purposes of Statutes of Limitation*, 28 Pac. L.J. 453, 457 (1997). Under the traditional conception of limitations rules, a statute of limitations prevented plaintiffs from bringing "stale" claims. *See Gabelli,* 133 S. Ct. at 1217 (citing *Rotella v. Wood,* 528 U.S. at 555) ("the basic policies of all limitations provisions: repose, elimination of stale claims, and certainty about a plaintiff's opportunity for recovery and a defendant's potential liabilities"). This theory posited that evidence would erode with time, undermining later attempts to adjudicate claims accurately. *Id.*

Courts quickly recognized, however, that imposing a time limit, chosen *ex ante*, will often artificially restrict the amount of information available to the court, or even prevent legitimate claims from arising in the first place. Yair Listokin, *Efficient Time Bars: A New Rationale for the Existence of Statutes of Limitations in Criminal Law*, 31 J. Legal

Stud. 99, 100 (2002). Courts developed a number of alternatives to ensure that plaintiffs could file lawsuits with enough information for the courts to adjudicate the claims. As Professor Epstein has noted:

> [O]ne possible escape from the dilemma is to hold, in a manner wholly consistent with ordinary usage, that injury and its manifestation mean the same thing. Another approach is to toll the statute of limitation until the date of discovery of the injury. … There is, I think, something to be said for a two-tiered statute of limitation that adds a fixed number of years for discovery, and then imposes an absolute ban on a cause of action, whether or not discovery has occurred.

Richard A. Epstein, *The Temporal Dimension in Tort Law*, 53 U. Chi. L. Rev. 1175, 1183 n. 19 (1986). *See also* Andrew J. Wistrich, *Procrastination, Deadlines, and Statutes of Limitation*, 50 Wm. & Mary L. Rev. 607, 667 (2008) (citation omitted).

The discovery rule is the most appropriate framework for claims arising from the DPPA because it is the rule that best furthers the purpose of the Act. The DPPA provides a cause of action for data privacy violations but does not provide for a breach notification system. *See* 18 U.S.C. § 2724. A victim of a DPPA violation must therefore discover the violation either by constantly checking with the DMV to ensure that her records remain secure, which is both impractical and

irrational, or wait until she is confronted with the consequences of a data breach.

Congress cannot have intended the DPPA to require constant vigilance from registered drivers. Such a requirement would overly burden registrants and discourage drivers from maintaining accurate records. Furthermore, DMVs could not support the costs of responding to repeated individual inquiries. Because drivers are dependent on DMV services in order to own, insure, and drive their cars, states are incentivized to provide DMV employees with minimal training. David Zaring & Elena Baylis, *Sending the Bureaucracy to War*, 92 Iowa L. Rev. 1359, 1381 (2007). DMV policies and procedures are predetermined, so DMV employees must only learn to execute these procedures. As a result, states tend to allocate minimal funding to DMVs. This system of low funding and minimal employee training self-perpetuates, as drivers have no alternative but to rely on DMVs. *Id.* Furthermore, this system may be beneficial for states, since it allows DMVs to execute their "massive mandate" by "maintaining a high volume, low budget operation." *Id.*

As a result, however, the resources required to add database breach oversight to this system would far eclipse a DMV's capacity. *See id.* at 1381 (explaining that since "[n]ondiscretionary standards for qualification are set by state legislatures and departments of transportation and applied in rote, assembly line fashion by low-level state-government bureaucrats on the spot," DMV functions are tightly restricted to "a narrow, specialized expertise—the registration, insurance, and safety of automobiles"). DMVs would need to not only develop a method for determining when a driver's data had been improperly accessed and train employees to make that determination, but also hire employees to respond to the numerous inquiries from concerned drivers. Such a system would be so costly and inefficient as to be ludicrous.

The DPPA was drafted to provide a remedy for drivers who have discovered that their privacy was violated by the improper use or disclosure of their records. As discussed in section I.B. above, the effects of privacy violations usually are not immediately observable. *See Gabelli,* 133 S. Ct. at 1222. Drivers are likely not to know the basis for their cause of action until the statute of limitations has expired. *See*

ITRC Fact Sheet 113. Moreover, once a statute of limitations has run, the cause of action immediately disappears. Andrew J. Wistrich, *Procrastination, Deadlines, and Statutes of Limitation*, 50 Wm. & Mary L. Rev. 607, 655 (2008). If the DPPA is to have any effect at all, it cannot include a statute of limitations that expires before the privacy violation manifests, nor can it require the prohibitively inefficient scrutiny of drivers. The rule that Congress anticipated for the DPPA must therefore have been the discovery rule.

CONCLUSION

Amicus respectfully requests this Court reverse the lower court's decision.

June 4, 2014

Respectfully submitted,

/s/ Marc Rotenberg

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

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 6,299 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 Word in 14-point Century Schoolbook style. This brief has been scanned for viruses and is virus free in compliance with 8th Cir. R. 28A(h).

Dated: June 4, 2014

/s/ Marc Rotenberg

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