Nos. 13-533, 13-539

IN THE

Supreme Court of the United States

ERIK H. GORDON,
Petitioner,
v.
SOFTECH INTERNATIONAL, INC., REID RODRIGUEZ, ARCANUM INVESTIGATIONS, INC., AND DAN COHN,
Respondents.

ARCANUM INVESTIGATIONS, INC., *ET AL.*
Petitioners,
v.
ERIK H. GORDON
Respondent.

On Petition for Writ of Certiorari to the United States Court of Appeals for the Second Circuit

BRIEF OF THE FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION AS *AMICUS CURIAE* IN SUPPORT OF PETITIONERS

JOSEPH V. DEMARCO
Counsel of Record
DAVID M. HIRSCHBERG
URVASHI SEN
KATE TSYVKIN
DEVORE & DEMARCO LLP
99 Park Avenue, Suite 330
New York, NY 10016
(212) 922-9499
jvd@devoredemarco.com

Counsel for Amicus Curiae Federal Law Enforcement Officers Association

November 26, 2013

WILSON-EPES PRINTING CO., INC. – (202) 789-0096 – WASHINGTON, D. C. 20002

TABLE OF CONTENTS

TABLE OF CONTENTS—Continued

TABLE OF AUTHORITIES

TABLE OF AUTHORITIES—Continued

TABLE OF AUTHORITIES—Continued

IN THE

Supreme Court of the United States

ERIK H. GORDON,

Petitioner,

v.

SOFTECH INTERNATIONAL, INC., REID RODRIGUEZ, ARCANUM INVESTIGATIONS, INC., AND DAN COHN,

Respondents.

ARCANUM INVESTIGATIONS, INC., *ET AL*.

Petitioners,

v.

ERIK H. GORDON

Respondent.

On Petition for Writ of Certiorari to the United States Court of Appeals for the Second Circuit

BRIEF OF THE FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION AS *AMICUS CURIAE* IN SUPPORT OF PETITIONERS

INTEREST OF *AMICUS CURIAE*[1]

The Federal Law Enforcement Officers Association ("FLEOA"), a volunteer organization founded in 1977, is the largest nonpartisan, nonprofit professional association exclusively representing federal law enforcement officers. FLEOA represents more than 25,000 uniformed and non-uniformed federal law enforcement officers from over 65 different agencies.

[1] No counsel for a party authored this brief in whole or part. Petitioner Erik H. Gordon has made a monetary contribution to fund the preparation and submission of this brief. S. Ct. R. 37.6. The parties were timely notified and they consented to this filing.

FLEOA is a charter member of the Department of Homeland Security Federal Law Enforcement Advisory Board; holds two seats on the Congressional Badge of Bravery Federal Board; and serves on the Executive Board of the National Law Enforcement Officers Memorial Fund and the National Law Enforcement Steering Committee. FLEOA provides a legislative voice for the federal law enforcement community and monitors legislative and other legal issues that may impact federal law enforcement officers.

FLEOA members have had substantial—and often tragic—experience with the dangers that are posed when personal information from Department of Motor Vehicles ("DMV") records falls into the wrong hands. FLEOA and its members thus have a strong interest in ensuring that the Driver's Privacy Protection Act ("DPPA"), which was enacted to protect this information from improper disclosure, is correctly interpreted and enforced, and that any inconsistencies among the various circuit courts—particularly on an issue as fundamental as the *mens rea* requirement of the statute—are swiftly resolved.

SUMMARY OF ARGUMENT

An individual's driver abstract contains highly personal information, including the individual's full legal name, date of birth, address and social security information, as well as an array of sensitive personal information including their height, eye color and medical conditions related to their ability to drive. Under the DPPA, state DMVs are permitted to disclose this information to parties with lawful needs, including needs relating to driver safety (such as manufacturer recalls) as well as in the course of investigating insurance claims. By virtue of its

sensitive nature, however, this information can *also* be misused by those seeking to harm, threaten, harass or intimidate the license holder.

Recognizing the potential for abuse, Congress enacted the DPPA to create a framework by which providers of personal information obtained from DMV records are permitted to disseminate this information for legitimate purposes, while those who provide such data without a permitted purpose are subject to civil and criminal penalties. The list of permissible purposes set forth in the DPPA was *not*, however, intended by Congress to operate as a mere formality that can be dispensed with through a "check box," insulating providers from liability, but rather to (1) impose an obligation on those providers not to disclose personal information for impermissible purposes and (2) penalize providers who disseminate driver records to those who could use those records for unlawful purposes. As such, the DPPA reflects Congress's judgment that (1) the personal information of an individual should be highly regulated and strongly safeguarded against unauthorized disclosure, and (2) those entities which lawfully possess and distribute DMV personal information should be held to a high standard of care in preventing impermissible disclosures of that information.

Unfortunately, under the current state of the law, there is a clear and crucial split among several circuits regarding what Congress intended for this standard of care to be with respect to data brokers or resellers of personal information.

Given the highly accurate nature of the personal information at issue here, combined with its nearly instantaneous accessibility through reseller websites, lack of clarity as to what actions trigger liability under

the DPPA endangers the lives of law enforcement officers and undermines the effective administration of the justice systems. Simply put, by virtue of their public service, law enforcement officials (along with first responders, members of the legislative and judicial branches and other public servants), as well as their family members face unique risks from acts of violence, harassment, extortion and identity theft perpetrated by those seeking to extract revenge or corrupt the functions of these public servants. Witnesses and crime victims are similarly at risk.

Under the circumstances, *Amici* respectfully submit that this is *precisely* the kind of case in which this Court's guidance is needed: a circuit split on a fundamental aspect of the DPPA, a statute that has a direct effect on public safety and privacy. Indeed, this Court previously determined that matters relating to the interpretation of certain subsections of the DPPA warranted review; so much more so when the matter at hand has to do with the *mens rea* requirement of the entire statute as a whole.

As such, *Amici* respectfully request that this Court grant Petitioner's petition for certiorari.

ARGUMENT

I. THE CURRENT STATE OF THE LAW PUTS CITIZENS AND LAW ENFORCEMENT OFFICERS IN DANGER

Although on its face the DPPA is a privacy statute, it serves an important anti-crime purpose. Part of the Violent Crime Control and Law Enforcement Act of 1994, the DPPA was enacted in response to a growing trend of violence and stalking victimizing individuals whose personal information had been acquired from DMV records. The most notorious of these crimes was

the 1989 murder of actress Rebecca Schaeffer, who was shot to death in her apartment doorway by Robert John Bardo—a crazed fan who had obtained her home address from California DMV records.[2] Particularly chilling also were the examples included in the testimony before Congress of David Beatty of the National Victim Center, who described numerous examples of the stalking, harassment, and murder of women facilitated by open access to DMV records.[3]

Recognizing the threat caused by unfettered access to individuals' personal information obtained from their DMV records, Congress determined that those records should not be disclosed *except* to those with a legitimate need for them. It embodied that intent in a statutory scheme designed to carefully limit disclosure. 18 U.S.C. § 2721(b).

However, the current conflict in governing law and the ensuing lack of clarity regarding liability under the DPPA endanger the welfare and privacy of every single individual who has applied for a license from, or registered a vehicle with, a state DMV. This danger is particularly palpable when it comes to public servants such as law enforcement officers (and their families), who are uniquely susceptible, by virtue of their job responsibilities, to being targeted by criminals who may misuse their personal information. Other persons involved in the administration of justice, such

---

[2] 138 Cong. Rec. H1785 (daily ed. Mar. 26, 1992) (statement of Rep. Moran).

[3] *Protecting Driver's Privacy Hearings, Subcomm. on Civil and Constitutional Rights of House Judiciary Comm.*, 103d Cong. (1994) (testimony of David Beatty, Dir. of Publ. Aff., Nat'l. Victim Ctr., 1994 WL 212822).

as crime victims, informants and other witnesses, are also subjected to similar risk.

A. DMV Databases Are Repositories of Extremely Accurate and High Quality Information That Citizens—Including Law Enforcement Officers and Their Families—Are Effectively Required to Provide to the DMV

At the time Congress passed the DPPA in 1994, millions of individuals were already required to disclose highly sensitive, personal information to state DMVs in order to obtain driver's licenses. As this Court noted in *Reno v. Condon*, 528 U.S. 141 (2000):

> State DMVs require drivers and automobile owners to provide personal information, which may include a person's name, address, telephone number, vehicle description, Social Security number, medical information, and photograph, as a condition of obtaining a driver's license or registering an automobile.

Id. at 143. Now, almost 20 years later, the amount of personal information collected by state DMVs is staggering, particularly with the enactment of the REAL ID Act of 2005, Pub. L. No. 109-13, 119 Stat. 302 (2005), which heightened the standards for state driver's licenses and ID cards. REAL ID Driver's Licenses and Identification Cards, 6 C.F.R. § 37.1 (2008).[4] As a result, state DMVs may collect a dizzying array of personal information. For example, the New

[4] States were required to become fully compliant with the REAL ID Act as of Jan. 15, 2013. 6 C.F.R. § 37.51 (2011).

York DMV provides a four-page list of documents that can be used to support a DMV application.[5]

Moreover, the vast majority of American adults—including law enforcement officers and their family members—have been required at one time or another to provide their personal information to the DMV. Put simply, for many individuals, driving, and therefore acquiring a driver's license, is a necessity of life. As such, the risk that their personal information will fall into the wrong hands extends to virtually every single citizen of the United States.

B. There Are No Reasonably Reliable Methods for Law Enforcement Officers to "Opt Out" of Providing This Information to the DMV

Unfortunately, unlike other mass repositories of personal information, such as the standard telephone directory, there is no reasonably reliable or cost-effective way to "opt out" and exclude one's personal information from inclusion in DMV records or from the

---

[5] These documents include, among others, the following: US Social security card; US passport or passport card; US military photo ID; Birth certificate; US Marriage or Divorce record; Court-issued name change decree; US Military dependent ID card; Federal or NYS W-2 tax forms; Bank statement, cancelled check, US cash card or valid major US credit card; US high school diploma or GED; US utility bill with name and address; Certificate of Residence; Credit card statement (original); 1098 or 1099 tax forms; Military orders still in effect; Property deed; Property or school tax bills or receipts for current year (with current address); Residential lease (issued within one year); Voter Registration Notification Card (issued within one year). *See* New York State Dep't of Motor Vehicles, Proofs of Identity, U.S. Citizenship and N.Y.S. Residence. NY DMV Proofs of Identity, U.S. Citizenship and NYS Residence, *available at* http://www.dmv.ny.gov/forms/id44edl.pdf.

databases maintained by private-sector resellers of those records. For example, the Internet website operated by Arcanum Investigations, Inc. ("Arcanum"), one of the resellers of Gordon's data in this case—www.docusearch.com—does not provide any opt-out options whatsoever. Another major data broker that provides information, including DMV records, to the public, www.USInfoSearch.com, similarly does not have any opt-out options. For its part, LexisNexis permits such opt-outs *only* if an individual is either (a) facing "a threat of death or serious bodily harm" or (b) is a victim of identity theft.[6] Of course, it bears noting that an individual who is facing either of these risks is likely someone who has already had their personal information compromised in some way, in which case such an opt-out is ineffective.

This circumstance is particularly problematic when the individual in question is a law enforcement officer or other public servant. Even in the case where an officer *could* provide the necessary documentation to demonstrate that he or she faces a threat on the job, he or she would have to submit documentation to every single data broker in existence in order for his or her personal information to remain secure.[7] This is

---

[6] *See* LexisNexis Opt Out Policy for KnowX and Accurint, *available at* http://www.lexisnexis.com/privacy/for-consumers/opt-out-of-lexisnexis.aspx ("LexisNexis Opt-Out").

[7] *See*, *e.g.*, LexisNexis Opt-Out, which states, "This opt-out policy only applies to personal information that is available through LexisNexis-owned databases. Please note opting-out of our databases will not prevent other companies or public record agencies from collecting or disseminating your personal information." While there are websites like www.privacyforcops.org that offer removal services, these are fee-based

impractical, unworkable and, arguably, impossible given the exponential rate of expansion of internet data brokerage businesses. Of course, it is an effectively impossible standard to meet when a law enforcement officer or other public servant lacks actual knowledge that he or she is facing a threat from some person or some group. The danger this poses is incontrovertible.

Moreover, even if each reseller of DMV records provided an opt-out mechanism which did not require a showing of past or imminent harm, as noted above, requiring individuals to track down each reseller to exercise that opt-out would shift the burden of protecting personal information from the resellers to the individual.

C. Improper Access to DMV Records Puts the Lives of Law Enforcement Officers and Other Public Servants at Significant Risk, Including Risk of Death or Serious Bodily Injury

As noted above, an individual's DMV records contain a range of highly sensitive personal information. In New York, for example, a driver's record contains the driver's name, address, date of birth, sex, height, eye color, and certain medical restrictions which affect the driver's ability to operate a motor vehicle.[8] While it is certainly true that states

---

websites and they are only able to offer such services for a handful of data aggregating websites.

[8] For example, various publicly available codes on a driver's DMV record indicate such things as "corrective lenses" (code "B"), "prosthetic device" (code "D"), "daylight driving only" (code "G") and "telescopic lens" (code "J"). *Driver License Restrictions*, http://www.dmv.ny.gov/olderdriver/restriction.htm.

do not currently make available all of the information that is included in DMV records upon request, this may change in the future in accordance with applicable laws, resulting in even more information becoming available to private citizens. Moreover, *Amici* respectfully submit that even if the *only* information available for release by state DMVs was names and addresses (a limitation not imposed by the DPPA), the array of possible misuses of even this limited body of information is truly staggering. Indeed, law enforcement officers are not the only persons at risk; first responders and public servants working in the military, homeland security and even the courts also face dangers from unauthorized access to personal information. So do private citizens—such as crime victims, informants and witnesses—who are essential to the administration of justice.

Targeted attacks against law enforcement officials and other public servants are an unfortunate reality. Only a few weeks ago, on November 1, 2013, a man with a deeply-held grudge against Transportation Security Administration ("TSA") officers entered Los Angeles International Airport, where he shot and killed a TSA officer at point blank range at a security checkpoint, while wounding two other TSA officers.[9] It is not difficult to imagine how much more easily this type of tragedy could occur when would-be attackers have access to highly accurate DMV personal information. For example:

---

[9] *See*, *e.g.*, LAX Shooting: The Latest on Shooter, Victims, and A Too Late Warning, available at http://www.cnn.com/2013/11/04/justice/lax-shooting/index.html (last visited November 5, 2013).

- A criminal attempting to intimidate or harass a crime victim, informant or fact witness could obtain his or her home address and telephone number and make threatening calls and visits to their home. Worse still, the criminal could kill or physically harm that person or a family member or loved one close to them.

- A person seeking to extract revenge against a public servant could use DMV personal information to steal their identity and wreak financial havoc on that person or their family members.

- A person with a grudge against law enforcement officials could wait outside the parking lot of a federal building and record the license plates of every car that enters or leaves—and then harass or do harm to those officials or their loved ones at home after obtaining their addresses.[10]

- Terrorists could utilize DMV personal information in a variety of ways to maximize harm to innocent civilians.[11]

Indeed, targeted attacks against law enforcement officials and other public servants using personal

---

[10] *Cf.* H.R. 3365, 103d Cong. (1993) (remarks of Rep. Moran) (citing, as one of the real-world examples involving misuse of DMV information, a ring of thieves in Iowa who scouted the long-term parking lot at an airport for luxury cars and then used DMV records to locate and rob unoccupied homes of drivers registered to those cars).

[11] FLEOA has specific, law-enforcement sensitive examples of this which it does not wish to place in the public domain. Should the Court, however, desire this information, FLEOA will make it available.

information obtained from databases are *not* hypothetical. For example:

> • Earlier this year, an individual who was convicted of two felonies in a jury trial, conducted LexisNexis searches on the two Assistant District Attorneys in his case, including searches involving driver's license numbers. He then located and murdered both prosecutors and one of their wives.[12]
>
> • Earlier this month, at the sentencing of a notorious member of the hacktivist collective "Anonymous," it was revealed that the defendant participated in a website attack and data dump which made public the home telephone number of a retired Arizona policeman. As a result of this, the retired policeman and his wife received *hundreds* of threatening and harassing telephone calls.[13]

In a world where digitized personal information can be accessed from anywhere and travels literally at the speed of light, it is imperative that courts have clarity on access rules to records under the DPPA, so that DMV personal information does not end up in the wrong hands.

---

[12] *See* The State of Texas v. Eric Lyle Williams, Warrant of Arrest and Detention, dated April 19, 2013, *available at* http://media.star-telegram.com/smedia/2013/04/18/15/33/c7bgo.So.58.pdf (last visited November 18, 2013).

[13] *See* Anonymous Hacker Jeremy Hammond Sentenced to Max Penalty of 10 Years in Prison, *available at* http://www.forbes.com/sites/andygreenberg/2013/11/15/anonymous-hacker-jeremy-hammond-sentenced-to-max-penalty-of-10-years-in-prison/ (last visited November 18, 2013).

D. Improper Access to DMV Records Can Undermine Law Enforcement and the Sound Administration of Justice

Equally troubling is the chilling effect that the misuse of personal information can have on the administration of justice. It is a reality of the Internet age that websites already exist which seek, in a variety of ways, to assist criminals and undermine law enforcement.[14] With ever-increasing frequency, criminals are also using social media to harm law enforcement officers and their mission[15] as well as to harass and intimidate informants and witnesses.[16] In such a world, it is essential that access rules to highly accurate DMV personal information—which can easily and quickly be combined with data about police officials, informants and witnesses obtained from social media—be clearly defined and understood.

II. THIS IS PRECISELY THE TYPE OF CASE THE SUPREME COURT SHOULD HEAR ON CERTIORARI

Amici respectfully submit that the case at hand is precisely the type of matter in which this Court's

---

[14] FLEOA does not wish to publicize the names of these websites, but can make a listing of them available to the Court should it so desire.

[15] *See*, *e.g.*, Officials Warn Facebook and Twitter Increase Police Vulnerability, *available at* http://www.foxnews.com/tech/2011/05/10/officials-warn-facebook-twitter-increase-police-vulnerability/ (last visited November 20, 2013).

[16] *See*, *e.g.*, Witness Harassment Has Gone Digital, And The Justice System Is Playing Catch-Up, *available at* http://www.abajournal.com/magazine/article/witness_harassment_has_gone_digital_and_the_justice_system_is_playing_catch/ (last accessed November 20, 2013).

guidance is essential. *First*, there is a genuine conflict here between several courts of appeals on an important federal question of national significance. For the reasons discussed above, this conflict has significant repercussions for almost every US citizen, especially those in law enforcement. *Second*, this Court has previously determined that matters relating to the interpretation of the DPPA are important enough to warrant review.

A. There Is a Circuit Split on an Important Federal Question

Rule 10(a) of the Rules of the Supreme Court states that this Court may consider granting certiorari on a matter in which "a United States court of appeals has entered a decision in conflict with the decision of another United States court of appeals on the same important matter . . . ." S. Ct. R. 10(a). The case at hand is clearly such a matter.

The DPPA is a federal statute that bars obtaining or disclosing drivers' personal information for any use not specifically authorized in the Act, and creates civil liability for "[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted." 18 U.S.C. § 2724(a).

As petitioner Erik H. Gordon ("Gordon") discusses in more detail in his Petition for Writ of Certiorari ("Gordon's Brief"), there are currently three different legal standards for determining liability under the DPPA. The Second Circuit below held that a reseller of personal information from a DMV record will only be civilly liable under the DPPA if it fails to exercise a "duty of reasonable inquiry" in determining whether the party requesting the information has a permissible

purpose, and that a voluntary act to obtain, disclose or use that information was not sufficient on its own to trigger liability. Gordon's Brief at 11-12; *Gordon v. Softech Int'l, Inc*., 726 F.3d 42, 56 (2d Cir. 2013). The Sixth Circuit, on the other hand, has held that actual knowledge of an impermissible purpose is required to trigger liability. Gordon's Brief at 11. Finally, the Third and the Seventh Circuits have held that only a voluntary or intentional act is required to trigger liability. *Id*.

The practical effect of the current state of the law to the case at bar is illuminating. In this case, Aron Leifer ("Leifer") submitted a request for information associated with Gordon's license plate number through www.docusearch.com, a website operated by Arcanum, by selecting "Insurance Other" from a drop-down menu to indicate his allegedly "permissible use." Arcanum forwarded this request to Softech International, Inc. ("Softech"), claiming only that the information was being requested for its own use as a private investigative agency. Softech provided the requested information to Arcanum, which then provided it to Leifer.[17] With respect to Arcanum, under these facts, liability in the Second Circuit only extends if the company did not take "reasonable care" to ensure that Leifer would not misuse Gordon's personal information; in the Sixth Circuit, liability is dependent on whether or not Arcanum actually "knew" that Leifer intended to misuse the personal information.

Not only will this current circuit split cause significant confusion in the industry, but there is very

---

[17] *Amici* respectfully assume the Court's familiarity with the facts of this case. For additional details, we respectfully refer the Court to Gordon's Brief at 7-10.

little incentive for Internet data brokers to go to any lengths to ensure the safety of the people whose personal information they sell, or to conduct any inquiries regarding their customers' or end users' true reasons for requesting that information. Unlike when Ms. Schaeffer was tragically killed (an era of mostly paper records), in the modern digital age, these data brokers can quite easily structure their businesses such that the most favorable law applies in any potential case relating to a violation of the DPPA. Under the Sixth Circuit's standard, in particular, they can then continue to dole out this personal information readily, in a matter of hours, as long as a customer or end user decides to "check the right box" in a drop-down menu. Even more troublingly, no decision at all is needed on sites where the *only* boxes that can be "checked" are the ones that parrot the DPPA's permissible use categories. Indeed, "drop down menu compliance" could provide a safe harbor to data brokers who turn a blind eye to this issue and their customers who specifically desire to harass law enforcement officials or otherwise impede the administration of justice.

As noted above, confusion in the law in this area has severe repercussions on the safety and privacy of every US citizen, and law enforcement officers in particular. It is precisely this type of situation—one that affects national safety, security and privacy—where national uniformity and clarity in the law is required. *Amici* respectfully submit that this Court would be hard-pressed to find another statute that not only affects almost every single US citizen, but also concerns one of the most fundamental aspects of our lives: our safety and security.

B. This Court's Previous Rulings Support Granting Certiorari Here

This Court recently reviewed, and granted, a petition for a writ of certiorari in another matter relating to the interpretation of a clause of the DPPA. Specifically, the Court addressed whether the solicitation of clients is encompassed under the DPPA's permissible purpose exception "for use in connection with any civil . . . proceeding in any Federal, State, or local court . . . including the service of process, investigation in anticipation of litigation, and the execution or enforcement of judgments and orders, or pursuant to an order of a Federal, State, or local court." DPPA (b)(4); *see Maracich v. Spears*, 133 S. Ct. 2191 (2013).

In granting certiorari in the *Maracich* matter, this Court implicitly acknowledged that clarity regarding the interpretation of the DPPA was essential. In its subsequent decision on the merits, this Court recognized the DPPA's fundamental purpose was "protecting an individual's right to privacy in his or her motor vehicle records" and that permitting the disclosure of personal information under Section (b)(4) "whenever any connection between the protected information and a potential legal dispute could be shown" would "undermine in a substantial way" this purpose. *Maracich*, 133 S. Ct. at 2193.

Amici respectfully submit that a matter of interpretation affecting the *mens rea* requirement of the DPPA warrants even greater consideration from this Court than resolving the issue in *Maracich*. As discussed in Section II.A, *supra*, liability under the DPPA turns entirely on how the word "knowingly" is interpreted. Under current jurisprudence, there are three conflicting interpretations of this. In order to

ensure that the DPPA serves its purpose of protecting individuals' rights to personal safety, it is imperative that this conflict be resolved as soon as possible.

CONCLUSION

Given the dangers that individuals involved in law enforcement and government regularly face as a result of their public service, allowing those dangers to be compounded by unauthorized access to their DMV personal information is irresponsible at best, and lethal at worst. It is therefore essential that this Court clarify the nature and scope of data brokers' responsibilities under the DPPA so that improper access to DMV personal information does not compromise the safety of those who we entrust with our lives.

The petition for a writ of certiorari should be granted.

Respectfully submitted,

JOSEPH V. DEMARCO
Counsel of Record
DAVID M. HIRSCHBERG
URVASHI SEN
KATE TSYVKIN
DEVORE & DEMARCO LLP
99 Park Avenue, Suite 330
New York, NY 10016
(212) 922-9499
jvd@devoredemarco.com

Counsel for Amicus Curiae Federal Law Enforcement Officers Association

November 26, 2013