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,

ABC CORPORATIONS 1 through 5, JOHN DOES 1 through 5,

Defendants-Cross-Defendants,

SOFTECH INTERNATIONAL, INC., REID RODRIGUEZ, ARCANUM INVESTIGATIONS, 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 IDENTITY THEFT RESOURCE CENTER AND THE FEDERAL LAW ENFORCEMENT OFFICERS ASSOCIATION AS *AMICI CURIAE* IN SUPPORT OF APPELLANT

DEVORE & DEMARCO LLP
Attorneys for Amici Curiae Identity Theft Resource Center and The Federal Law Enforcement Officers Association
99 Park Avenue, Suite 330
New York, New York 10016
(212) 922-9499

CORPORATE DISCLOSURE STATEMENTS

Pursuant to Rules 26.1 and 29(c)(1) of the Federal Rules of Appellate Procedure:

The Identity Theft Resource Center certifies that it is a privately-held 501(c)(3) non-profit corporation organized on behalf of its members; that it has no parent or subsidiary corporations; and that no publically-held company owns 10% or more of its stock.

The Federal Law Enforcement Officers Association certifies that it is a privately-held 501(c)(3) non-profit corporation organized on behalf of its members; that it has no parent or subsidiary corporations; and that no publically-held company owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases:

Statutes:

Other Authority:

STATEMENT OF INTEREST OF *AMICI CURIAE*

The Identity Theft Resource Center ("ITRC"), a 501(c)(3) non-profit organization, was originally formed as VOICES (Victims of Crimes Extended Services) in 1999 to support victims of identity theft in resolving their cases, and to broaden public awareness and understanding of identity theft. The ITRC's long-standing mission has been to provide best-in-class assistance at no charge to victims of identity theft throughout the United States. In addition to victim services, it is the ITRC's on-going mission to educate consumers, corporations, government agencies and other organizations on best practices for fraud and identity theft prevention, detection, reduction, and mitigation.[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. 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

[1] Pursuant to Federal Rule of Appellate Procedure 29(c)(5) and Second Circuit Rule 29.1(b), *amici* state that no counsel for a party has written this brief in whole or in part. Appellant Erik H. Gordon has made a monetary contribution that was intended to fund the preparation and submission of this brief.

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.

SUMMARY OF ARGUMENT

Appellees Softech International, Inc. ("Softech") and its Chief Operating Officer, Reid Rodriguez, and Arcanum Investigations, Inc. ("Arcanum") and its owner, Dan Cohn (collectively the "Reseller Defendants"), claim that they are exempted from liability under the Driver's Privacy Protection Act ("DPPA") because they did not have actual knowledge that Aron Leifer intended to use the information he obtained from them for a purpose not permitted by the Act. The Reseller Defendants further assert that their disclosure was made for a permissible purpose because Leifer "certified" to Arcanum that he had a permissible purpose for obtaining the data. These arguments, however, conflict both with a plain reading of the statute itself and with Congress's intent in passing the DPPA.

An individual's driver abstract contains highly personal information regarding a driver, including his or her full legal name, date of birth and address as well as an array of sensitive personal information including their height, eye color

and medical conditions related to their ability to drive. It also contains a person's driving record, including violations, suspensions, accidents and dates of licensure and expiration. Under the DPPA, the Department of Motor Vehicles ("DMV") is 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 threaten, harass or harm the license holder. Recognizing the potential for this abuse, Congress enacted the DPPA to create a framework by which providers of personally identifiable information ("PII") obtained from DMV records are permitted to do so 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 merely as a formulaic "check box" insulating providers from liability, but rather to impose an obligation on those providers not to disclose PII for impermissible purposes and to penalize dissemination of driver records to those who could use that those records for unlawful purposes. As such, the DPPA reflects Congress's judgment – one echoed in a broad array of similar identity-protective laws – that (1) the PII of an individual should be highly regulated and strongly safeguarded against unauthorized disclosure, and (2) those

entities which lawfully possess PII information should be held to a high standard of care in preventing impermissible disclosures of that PII.

Amici respectfully submit that to allow a customer's single click of a mouse to provide insulation from liability under the DPPA is to encourage willful blindness on the part of the entities we trust to protect our PII. This Court should recognize congressional intent and protect public safety by rejecting Reseller Defendants' assertion that they may shirk their responsibilities under the DPPA in this manner. Holding data brokers such as the Reseller Defendants responsible for their unlawful disclosures would *not* prevent legitimate users of DMV records from obtaining those records. Rather, it would encourage the implementation of policies and practices that would reduce the likelihood that those records fall into the wrong hands.

ARGUMENT

I. THE DISTRICT COURT ERRED IN INTERPRETING THE DPPA AS PRECLUDING LIABILITY ON THE PART OF DATA RESELLERS WHO RELY ON A PURCHASER'S ALLEGED PERMISSIBLE PURPOSE IRRESPECTIVE OF WHETHER THE PURCHASER IN FACT HAS A PERMISSIBLE USE

A. The District Court's Reliance on Roth v. Guzman *Was Misplaced*

In *Gordon v. Softech International, Inc.*, the District Court held that the DPPA's enforcement provisions could not be read as imposing liability on data

resellers for the misuse of their customers when those customers had misrepresented their intended use of the disclosed data. 828 F. Supp. 2d 665, 676 (S.D.N.Y. 2011). The District Court reached this conclusion based largely on the Sixth Circuit's holding in *Roth v. Guzman*, 650 F.3d 603, 609-12 (6th Cir. 2011), which held that Ohio state officials could not be held liable under 42 U.S.C. § 1983 42 U.S.C. § 1983for the disclosure of drivers' PII in violation of the DPPA when the vendor to which the state officials disclosed the data had misrepresented its intended use. *Roth*, however, was not concerned chiefly with whether the officials violated the DPPA. Rather it principally dealt with the issue of the qualified immunity of state officials and whether the class plaintiffs drivers' rights under the DPPA were "clearly established." *Id.* at 612-14. The defendants in the instant case have no similar immunities under the law.

The District Court also failed to properly address the mental state required for a violation of the DPPA. In its ruling, the Court *only* considered strict liability and actual knowledge standards for a reseller's awareness of its customers' intended misuse. This, however, is a false dichotomy. By failing to consider intermediate standards – including negligence, recklessness, willfulness and willful blindness – the Court, in rejecting strict liability, essentially read a specific intent requirement into the statute where none exists. *Amici* respectfully submit that this was error.

B. Congress Intended the Liability Provisions of the DPPA to be Interpreted as Imposing an Affirmative Obligation on Resellers to Determine the True Purpose of Their Customers

Although on its face the DPPA is a privacy statute, it serves an important anti-crime purpose. The DPPA was enacted in 1994 in response to a trend of violence and stalking victimizing individuals whose PII had been acquired from DMV records. The most notorious of these crimes was the 1989 murder of the 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] Other examples involving misuse of DMV information cited by Congress in passing the DPPA included the activities of an antiabortion group in Minnesota who used DMV records to harass an abortion provider in that state, including by spreading leaflets to the provider's child's friends at school harassing those children,[3] and 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.[4] Particularly chilling were the examples included in the testimony before Congress of David Beatty of

---

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

3 *Id*.

4 H.R. 3365, 103d Cong. (1993) (remarks of Rep. Moran).

the National Victim Center, who described numerous examples of the stalking, harassment, and murder of women facilitated by open access to DMV records.[5]

Recognizing the threat caused by unfettered access to individuals' PII and obtained from drivers' records, and seeking to balance that concern against the legitimate need of certain parties to have access to 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 the uses for which such information may be disclosed. 18 U.S.C. § 2721(b). Congress made clear its intent that the burden of ensuring the permissibility of disclosures be borne by data brokers by imposing a record keeping obligation on them to maintain a list of not only the people to whom they disclosed the data, *but also for what purpose the disclosure was made*. 18 U.S.C. § 2721(c). Of course, such a requirement would be nonsensical if records contained in that list were nothing more than compilations of potentially fictitious box checking.

Data brokers, including Reseller Defendants, who sell DMV data through automated Internet services that simply require their customers to select a

---

[5] *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).

"purpose" from a pre-defined list of options and then make no efforts whatsoever to ensure that the representations made by their customers are truthful clearly frustrate Congress's intent in enacting the DPPA. The families of Ms. Schaeffer and other crime victims would certainly have found no solace had they been informed that, prior to unlawfully obtaining their loved ones' addresses, their stalkers had clicked a drop down menu selection labeled "Insurance – Other," and that the providers did *nothing* to verify what this meant. *Amici* respectfully submit that this Court should reject drop down menu immunity for data brokers and apply the DPPA in a manner consistent with Congress's victim-protective purpose.

C. The DPPA Does Not Precondition a Reseller's Liability on Its Actual Knowledge of a Purchaser's Impermissible Purpose

The District Court held that in order to be held liable under the DPPA, a reseller must have actual knowledge of its customer's impermissible use. 828 F. Supp. 2d 665, 676. The structure of the DPPA, however, clearly indicates that liability of a reseller of DMV records is not predicated on their knowledge of the end user's actual purpose. Rather, it is the same as the end user's. That is because section 2722(a) makes no distinction between the mental state required by the person who obtains PII from a motor vehicle record and one who discloses it. Indeed, the statue on its face applies equally to those who "obtain" and those who "disclose" PII. 18 U.S.C. § 2722(a). Had Congress envisioned a narrower scope

of liability for resellers than for end users, it could have done so by treating them separately – which it did not. At least one analogous federal statute, however, does so. The Federal Telephone Records and Privacy Protection Act, which prohibits the disclosure of telephone records (including name and address) imposes criminal penalties against those who wrongfully obtain confidential phone records information. 18 U.S.C. § 1039(a).[6] Penalties for wrongful *disclosures*, however, are provided in a separate section. 18 U.S.C. § 1039(b).[7] By including penalties for both resellers and end users in the same section of the DPPA, Congress indicated its intent that, in the same factual circumstances, each of those two parties should be treated the same.

Even if this Court is unwilling to read the statute literally and apply no knowledge requirement on the part of a reseller to the actual use of the purchaser, a standard which requires actual knowledge is clearly too narrow. The District Court, however, apparently did not consider *any* standards between specific intent and strict liability. As discussed more fully below, sound policy concerns dictate that with respect to the actual intended use of disclosed PII, data brokers be

---

[6] Section 1039(a) imposes fines and imprisonment of up to 10 years for those who knowingly and intentionally obtain confidential phone records by fraudulent means.

[7] Section 1039(b) imposes fines and imprisonment of up to 10 years for those who knowingly and intentionally sell or transfer confidential phone records in violation of the statute.

required to conduct at least some reasonable inquiry into that purpose. At a minimum, resellers should be required to verify the identity of the person making the request and take basic steps to confirm the truthfulness of the requester's stated purpose. To hold otherwise is to encourage willful blindness as a defense to liability. *Amici* respectfully submit that even if this Court does not hold that a strict liability standard is applicable to the statute, it remand the case with an appropriate instruction to the District Court to apply a standard which imposes a reasonable duty on resellers to conduct at least some minimal investigation.

II. THE DISTRICT COURT FAILED TO APPRECIATE SOUND POLICY REASONS FOR READING THE DPPA TO FIND LIABILITY ON THE PART OF RESELLERS WHERE PURCHASERS HAVE NO PERMISSIBLE PURPOSE

Three policy concerns underlying Congress's enactment of the DPPA also support a reading of the Act which holds data resellers liable for the misuse of disclosed PII. *First*, the harm done to innocent victims as a result of the improper disclosure of PII is often severe. *Second*, individuals seeking to protect their privacy and security have no way to opt-out of the sharing of their PII with the DMV if they want to legally operate a motor vehicle. *Finally*, interpreting the DPPA in a manner urged by *Amici* is consistent with – and gives full effect to – the corpus of other congressionally-enacted statutes that safeguard PII.

As noted above, an individual's DMV records contain a range of highly sensitive PII. 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] It also includes that person's driving history, including violations, suspensions, accidents and dates of licensure and expiration. The array of possible misuses of this body of information is truly staggering. An angry ex-husband could use address records to locate and then threaten his ex-wife. A burglar could scout long-term parking at an airport to identify homes likely to be unattended at night – and then rob those homes. A person with a grudge against law enforcement 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. Moreover, in some states, where police officers do not have computer terminals in their cars that can access photographs of drivers, information thieves who are stopped for traffic violations could claim to have "forgotten" their driver's license and provide the seemingly legitimate information of the innocent victim of their theft. When the victim fails to respond to any ticket, a warrant may very well issue

[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.

for their arrest. Indeed, cases of criminal identity theft are not a rare occurrence. Since January 2010, the Identity Theft Resource Center victim advisors have handled 1,569 criminal identity theft cases out of 14,829 total identity theft cases. Although these cases represent approximately 11% of the ITRC case load, they also represent the most difficult cases for the victims. All of these not-so-hypothetical examples underscore the need for robust protection of PII in DMV databases *and* a corresponding interpretation of the DPPA which gives effect to such robust protections.

Beyond the possibility of misuse, however, strict protection of DMV PII is also warranted due to the unique characteristics of the driver's license itself. For many individuals, driving, and therefore acquiring a driver's license, is a necessity of life. As such, the vast majority of American adults have been required at one time or another to provide their PII to the DMV. Furthermore, unlike other mass repositories of PII, such as the telephone directory, there is no easy or cost-effective way to "opt out" and exclude one's PII from inclusion in DMV records. Nor should there be: it is, after all, vitally important to driver safety that insurance claims are able to be properly investigated and that vehicular safety recalls are correctly delivered – tasks which necessarily depend on the maintenance and disclosure of accurate drivers' records. Given ever-growing fears of identity theft, and the real need of certain people and classes of people to protect themselves

against the threats posed by stalkers, to allow the only national statute safeguarding DMV PII to be easily circumvented by data brokers could tempt such drivers to provide false information to the DMV. *Amici* submit that putting such drivers to the dilemma of either risking disclosure of their PII by an unscrupulous data broker or submitting false information to the DMV– a crime in New York makes no sense.[9]

These problems can best be avoided by imposing upon data broker an obligation to verify that the purposes for which they disclose driver's records are *in fact* permissible under the DPPA. Although these entities would incur some additional burdens in doing so, the benefit of preventing stalking, harassment, identity theft, and other criminal acts would be well worth the cost. Furthermore, the data brokers serve as a necessary conduit through which disclosed driver's records flow. By virtue of this unique position, they are uniquely situated to avoid the evils described above at the least cost and can therefore best serve as gatekeepers who protect the privacy interest of the American driver.

Finally, interpreting the DPPA in a manner (at the minimum) which holds data brokers to a reasonable degree of care concerning those they disclose information to is in harmony with congressionally mandated procedures in similar

[9] *See, e.g.*, New York Penal Law Section 175.30 (describing crime of "Offering a False Instrument for Filing in the Second Degree").

situations. Congress has created an elegant framework of laws and regulations safeguarding PII and the laws which make up this framework *regularly* require entities holding PII to implement robust practices designed to prevent unauthorized disclosure. For example, the Gramm-Leach-Bliley Act's "Safeguards Rule" expressly requires covered financial institutions to have "policies, procedures, and controls in place to *prevent* the unauthorized disclosure of customer financial information" and to detect and deter attempts to solicit customer information such as names and addresses under false pretenses. 15 U.S.C. § 6825 (emphasis supplied). Similarly, the Health Insurance Portability Act's ("HIPAA") "Privacy Rule" imposes exacting standards to protect the privacy of personal health information. *See*, *e.g.*, 45 C.F.R. Parts 160, 162 and 164.

Beyond simply dictating the security standards that must be applied to protect PII in various databases, other federal statutes which protect PII also routinely provide *penalties* for improper disclosure. In particular, Congress has enacted an array of laws which punish private parties responsible for improper PII dissemination even in the absence of the intent to accomplish the prohibited disclosure or actual knowledge of facts which render disclosure impermissible. The breadth of these statutes and the variety of industries they regulate makes crystal clear that congressional intent to strictly regulate the disclosure of PII by private sector actors is the norm. It also demonstrates that the DPPA should not be

interpreted by this Court to create a loophole to the protections afforded by these laws. A non-exhaustive listing of pertinent PII-protective federal laws includes the following:

HIPAA: In the context of health care, disclosures of PII under HIPAA are only permitted with an authorization which specifies what information is to be released, to whom it is to be released, and for what permitted purpose the release is to be used. 45 C.F.R. § 164.508(c)(1). A HIPAA- covered entity who knowingly discloses individually identifiable health information in violation of HIPAA may be subject to criminal penalties, 42 U.S.C. § 1320D-6, and civil penalties exist even where the violator "did not know (and by exercising reasonable diligence would not have known)" that they were violating the Act. 42 U.S.C. § 1320D-5(a)(1)(A).

Fair Credit Reporting Act ("FCRA"): In the context of consumer reporting, federal law makes clear that FCRA-covered entities may only release consumer report information (which includes PII) to those whom they have reason to believe will use the information for a permissible purpose listed in the statute. 15 U.S.C. § 1681b. To prevent reliance on drop-down menu verification, credit reporting agencies are required to have "reasonable procedures" in place to limit requests for PII for impermissible purposes, including making "a reasonable effort to verify the identity of a new prospective user and the uses certified by such prospective user

prior to furnishing such user a consumer report." 15 U.S.C. § 16813(a). FCRA's enforcement provisions provide penalties for willful, knowing, and negligent noncompliance. 15 U.S.C. § 1681(n), (o).

Family Educational Rights and Privacy Act ("FERPA"): In the context of educational records, FERPA places stringent requirements on educational institutions' ability to release student records (including PII) without parental consent. Moreover, just as is required by the DPPA in section 2721(c), under FERPA, educational institutions are required to keep detailed records of all disclosure requests. *See* 34 C.F.R. § 99.32. Schools which permit the unauthorized release of students' PII can face penalties from the Department of Education, including the loss of federal education funding. 20 U.S.C. § 1232g(b)(1). Notably, the U.S. Department of Education has interpreted FERPA's mandate to secure students' PII as imposing strict liability on providers for the subsequent misuse of that data. For example, in a letter to a school district which discussed the use of third-parties to handle academic records, the Department stated "the agency or institution that outsources services under these requirements remains *completely responsible* for its service provider's compliance with

applicable FERPA requirements and liable for any misuse of protected information."[10]

Federal Telephone Records and Privacy Protection Act: In the context of telecommunications law, the Federal Telephone Records and Privacy Protection Act ("FTRPPA") makes clear that carriers may not sell or release "confidential phone records" information (which include PII) without the authorization of the customer to whom they pertain. 18 U.S.C. § 1039(b)(1). The law provides criminal penalties for carriers who either "knowingly and intentionally" sell or transfer PII without authorization, or provide such information "knowing or having reason to know such information was acquired fraudulently." *Id*.

Video Privacy Protection Act ("VPPA"): The VPPA provides a list of permissible conditions for disclosure of PII in a similar manner as does the DPPA. 18 U.S.C. § 2710(b)(2).[11] The VPPA provides a consumer a civil remedy against a covered person who "knowingly discloses, to any person, personally identifiable

---

[10] Letter from LeRoy S. Rooker, Director, Family Policy Compliance Office, U.S. Dep't. of Education, to Jeanne-Marie Pochert, Deputy Assistant General Counsel, Clark County School District Legal Dep't. (June 28, 2006), *at* http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/clarkcty062806.html (emphasis supplied).

[11] Disclosure is permitted if made (A) to the consumer or (B) upon his or her written consent, (C) to a law enforcement agency with a warrant, (D) to any party if the consumer has been provided a clear and conspicuous manner in which to opt out, (E) if incident to the ordinary course of business of the video tape service provider, and (F) pursuant to a court order. 18 U.S.C. § 2710(b)(2)(A)-(F).

information" concerning a consumer without mention of whether the covered person knows of the attendant circumstances which render the disclosure impermissible. 18 U.S.C. § 2710(b)(1).

As demonstrated above, across a range of circumstances, Congress has expressed its judgment that databases of individuals' PII should be closely guarded, and that the burden – including the risk of civil or criminal penalties – of protecting that information should be borne by the entities which maintain it. It has, across a range of industries and data sets, enacted penalties for unauthorized releases of PII calibrated to the culpability of the party releasing data and ranging from strict liability to negligence, knowledge and willfulness. So too does the DPPA, containing graduated penalties based on strict liability (or negligence), 18 U.S.C. § 2724(a), as well as reckless or willful disregard of the law. 18 U.S.C. § 2724(b)(2). The District Court decision ignored this carefully calibrated regime of PII protections and, in so doing, undermined the careful framework created by Congress to protect PII from wrongful disclosure and misuse. *Amici* respectfully submit that the DPPA should be interpreted in harmony with these PII-protective laws and that the District Court's ruling to the contrary should be rejected.

CONCLUSION

The DPPA was intended to strike a balance between the legitimate need of certain parties to have access to the personal information concerning drivers contained in DMV records and the protection of drivers' safety and privacy from those who would misuse such data. Data brokers, such as those operated by Reseller Defendants subvert the latter protection by attempting to comply with the Act in a nominal, but totally ineffective, manner. In the view of *Amici* a correct balance of interests can best be accomplished by requiring data brokers to implement reasonable practices to avoid prohibited disclosures of drivers' records – and by holding those who fail to do so liable for the harm they cause.

Dated: June 13, 2012

/s/ Joseph V. DeMarco
JOSEPH V. DEMARCO

DEVORE & DEMARCO LLP
Attorneys for Amicus Curiae
Identity Theft Resource Center
99 Park Avenue, Suite 330
New York, New York 10016
(212) 922-9499

CERTIFICATE OF COMPLIANCE

Pursuant to Rule 32 of the Federal Rules of Appellate Procedure, I certify that:

1. This brief complies with the type-volume limitation of Rule 32(a)(B) of the Federal Rules of Appellate Procedure because this brief contains 4,252 words, excluding the parts of the brief exempted by Rule 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Rule 32(a)(5) and the type style requirements of Rule 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft© Word 2007 in 14-point Times New Roman.

Dated: June 13, 2012

/s/ Joseph V. DeMarco
JOSEPH V. DEMARCO

CERTIFICATE OF SERVICE

I hereby certify that on June 13, 2012, a true and correct copy of the foregoing Brief by the Identity Theft Resource Center and the Federal Law Enforcement Officers Association as *Amicus Curiae* Supporting Appellant Erik H. Gordon was served on all counsel of record in this appeal via CM/ECF pursuant to Second Circuit Rule 25.1(h)(1)(2).

Dated: June 13, 2012

/s/ Joseph V. DeMarco
JOSEPH V. DEMARCO