

NO. 10-1193

**IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT**

**LISA M. GRACZYK, MATTHEW M. JORGE,
AND BRIAN WILLINGHAM, INDIVIDUALLY AND ON
BEHALF OF ALL OTHERS SIMILARLY SITUATED,**

Plaintiffs-Appellants,

v.

**WEST PUBLISHING CORP.,
A MINNESOTA CORPORATION,**

Defendant-Appellee.

On Appeal from a December 23, 2009 Order of
the United States District Court for the Northern District of Illinois,
Eastern Division, Case No. 1:09-cv-04760
The Honorable Judge Robert W. Gettleman

**Amicus Brief of the Coalition for Sensible Public Records Access and the Consumer
Data Industry Association in Support of Defendant-Appellee and for the Affirmance of the
District Court's Judgment Dismissing Plaintiffs-Appellants' Claims**

**RONALD I. RAETHER, JR.
OHIO BAR NUMBER 0067731
FARUKI IRELAND & COX P.L.L.
500 COURTHOUSE PLAZA, S.W.
DAYTON, OHIO 45402
(937) 227-3700**

**Counsel for Amicus Curiae,
The Coalition for Sensible Public Records Access and
The Consumer Data Industry Association**

CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: No. 10-1193

Short Caption: Graczyk, et al. v. West Publishing Corp.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party or amicus curiae, or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statement be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in front of the table of contents of the party's main brief.

Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.

[] PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):

Coalition for Sensible Public Records Access (amicus curiae)
Consumer Data Industry Association (amicus curiae)

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:

Faruki Ireland & Cox P.L.L.

(3) If the party or amicus is a corporation:

i) Identify all its parent corporations, if any; and

ii) list any publicly held company that owns 10% or more of the party's or amicus' stock:

Attorney's Signature: _____ Date: _____

Attorney's Printed Name: Ronald I. Raether, Jr.

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). Yes X No _____

Address: 500 Courthouse Plaza, S.W., 10 N. Ludlow St., Dayton, OH 45402

Phone Number: (937) 227-3733 Fax Number: (937) 227 -3717

E-Mail Address: rraether@ficlaw.com

rev. 01/08 AK

TABLE OF CONTENTS

I.	Governmental Agencies and Private Businesses Rely on Information Providers to Offer Benefits that the States Cannot	4
A.	Commercial Information Providers Offer Significant Benefits to the Public	4
B.	Information Providers Have Tools Essential to Achieving the above that States Cannot or Do Not Provide.....	9
II.	The Bulk Obtainment of Motor Vehicle Records by Information Providers Is a Long-Standing and Accepted Practice.....	13
III.	There Are Sufficient Existing Controls to Achieve Balance between Privacy and Accessibility of DPPA Information for Permissible Uses.....	15
A.	Entities that Obtain DPPA Information in Bulk for Resale for DPPA-Permitted Uses Protect that Information from Improper Use	16
B.	For Some Information Providers, the GLBA Safeguards Rule Further Protects DPPA Information.....	18
IV.	Conclusion	18

TABLE OF AUTHORITIES

CASES

<i>Collier v. Dickinson</i> , 477 F.3d 1306 (11th Cir. 2007), <i>cert. denied</i> , 552 U.S. 1096, 128 S. Ct. 869 (U.S. 2008).....	16
<i>Columbia Gas Transmission Corp. v. Federal Power Commission</i> , 530 F.2d 1056 (D.C. Cir. 1976).....	13
<i>Kohl's Food Store, Inc. v. Hyland</i> , 32 F.3d 1075 (7th Cir. 1994).....	13
<i>S.J. Groves & Sons Co. v. Occupational Safety and Health Review Commission</i> , 648 F.2d 95 (2d Cir. 1981).....	13
<i>Yonter v. Aetna Finance Co.</i> , 777 F. Supp. 490 (E.D. La. 1991).....	13

STATUTES

16 C.F.R. § 314.3(a)	18
16 C.F.R. § 314.3(b).....	18
18 U.S.C. § 2721 <i>et seq</i>	2
18 U.S.C. § 2721(c).....	15, 17, 18
18 U.S.C. § 2723(b).....	16
18 U.S.C. § 2724	17

MISCELLANEOUS

139 Cong. Rec. S15962 (Nov. 17, 1993).....	5,13
140 Cong. Rec. H2518 at 2523 (Apr. 20, 1994)	14
67 Fed. Reg. 36484-485 (May 23, 2002).....	18

<u>Prepared Statement of Louis J. Freeh, Director, FBI before the Senate Appropriations Committee, Commerce, Justice and State, the Judiciary and related Agencies Subcommittee, 1999 WL 170227 (Mar. 24, 1999)</u>	6,11,14
<u>Brief of the State of Texas as Amicus Curiae in Support of Defendants, Taylor v. Acxiom Corp., Case Nos. 08-41083, 41180, 41232</u>	8
<u>Testimony of James Ho for State of Texas, Taylor v. Acxiom Corp., Case Nos. 08-41083, 41180, 41232 (Nov. 4, 2009)</u>	9
<u>October 9, 1998 letter from R. McFetridge, Special Counsel of the Assistant Attorney General, Civil Division, to P. Sacks</u>	15
<u>Federal Trade Commission, Prepared Statement before the Senate Committee on the Judiciary, Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use (Apr. 13, 2005), available at http://www.ftc.gov/os/testimony/050413personaldata.pdf (last viewed April 6, 2010)</u>	5
<u>CSPRA, Public Benefits from Open Public Records, available at http://www.cspra.us/downloads/publicbenefits.pdf</u>	6,8
<u>Federal Bureau of Investigation, <i>The Beltway Snipers</i>, available at http://www.fbi.gov/page2/oct07/snipers102207.html</u>	6,7
<u>Federal Bureau of Investigation, <i>The Beltway Snipers</i>, available at http://www.fbi.gov/page2/oct07/snipers102407.html</u>	6,7
<u>Fox News, May 4, 2010, <i>Times Square Car Bomb Suspect Faces Terrorism Charges After Admitting to Plot</i>, available at http://www.foxnews.com/politics/2010/05/04/times-square-car-bomb-suspect-faces-terrorism-charges-admitting-plot/</u>	7
<u>National Center for Missing and Exploited Children, <i>Missing Children Success Stories</i>, available at www.missingkids.com/servlet/pageservlet?LanguageCountry=en_US&PageId=3518</u>	7
<u>July 14, 2007, Jennifer Sullivan and Maureen O’Hagon, <i>Seattle Times</i>, <i>Police Seek to Tie Other Cases to Girl’s Death</i>, available at http://seattletimes.nwsourc.com/html/localnews/2003788864_linnik14m.htm</u> 1	8
<u>CSPRA, Consumer Benefits from Public Records, available at http://www.cspra.us/downloads/consumerbenefits.pdf</u>	9

Personal Information Acquired by the Government from Information Resellers: Is There Need for Improvement?; Joint Hearing before the Subcomm. On Commercial and Administrative Law, Prepared Statement of Stuart K. Pratt, President and CEO of CDIA, 109th Cong. No. 109-08 (Apr. 4, 2006), available at <http://www.access.gpo.gov/congress/house/pdf/109hrg/26912.pdf> 10

The Privacy Office, Department of Homeland Security, Privacy and Technology Workshop, Official Transcript (Sept. 8-9, 2005) (comments of Chris Swecker, Assistant Director of the Criminal Investigative Division for the FBI), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_wkshop_09-2005_transcript_panel1.pdf..... 11

May 2006, Rob McKenna, Attorney General of Washington and U.S. Department of Justice Office of Juvenile Justice and Delinquency Prevention, *Case Management for Missing Children Homicide Investigation*, available at http://www.missingkids.com/en_US/documents/homicide_missing.pdf..... 11

The Privacy Office, Department of Homeland Security, Privacy and Technology Workshop, Official Transcript (Sept. 8-9, 2005) (comments of Grace Mastalli Principal Deputy Director for the Information Sharing and Collaboration Program at DHS), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_wkshop_09-2005_transcript_panel1.pdf..... 12

Lynn Peterson and Genie Tyburski, *The Truth about Big Brother Databases* (Oct. 3, 2002), available at www.cspra.us/downloads/BigBrotherDatabases.htm 17

IDENTITY, INTEREST AND AUTHORITY OF AMICUS CURIAE

The Consumer Data Industry Association (“CDIA”) is an international trade association, founded in 1906, and headquartered in Washington, D.C. CDIA is the largest trade association of its kind in the world. Its membership includes more than 300 consumer information companies that provide various products and services to governmental and business entities for, among other things, law enforcement, risk management, and fraud prevention purposes. In its more than 100-year existence, CDIA has worked with the United States Congress and with state legislatures to develop laws and regulations governing the collection, use and dissemination of information pertaining to individuals. CDIA also establishes industry standards and provides business and professional education for its members.

The Coalition for Sensible Public Records Access (“CSPRA”) is a non-profit organization dedicated to promoting the principle of open public records access to ensure that consumers and businesses have the freedom to collect and use public record information for legitimate personal and commercial benefit. CSPRA seeks to educate policymakers and the public about the beneficial and critical uses of public records information and the unintended consequences that could result from legal restrictions that limit or otherwise impede access to public records information. In connection with its educational mission, CSPRA (a) prepares white papers regarding various public records issues, (b) is involved in relevant legislative and rule-making comment processes, and (c) sponsors activities designed to foster a more thoughtful debate about how public record access should be balanced with privacy concerns.

Members of CSPRA and CDIA include information providers that have for decades served governmental agencies and business entities by obtaining and providing access to information pertaining to individuals for socially beneficial uses, including information contained in motor

vehicle records, which are disclosed for one or more of the permissible uses defined by the Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. § 2721 *et seq.* The members of CSPRA and CDIA offer unique applications and tools to make this information available in a manner essential to achieve a variety of DPPA-permitted governmental and business purposes, including (a) to prevent identity theft and fraud, (b) to trace non-custodial parents to enforce child support orders, (c) to locate and recover missing children and adults, and (d) to assist law enforcement officials in locating and apprehending fugitives.

As the states, industry, law enforcement, and other governmental agencies have recognized for the past sixteen years, Congress understood the crucial role of information providers and, in enacting the DPPA, sought to achieve a balance between privacy and the legitimate business and governmental uses enumerated in the DPPA. And for the last sixteen years, the threat of monetary penalties available under the DPPA has given the information provider industry incentive to protect information in motor vehicle records and to disclose that information only for the purposes permitted by the statute. Plaintiffs now challenge these long-standing practices—not on the basis of any actual injury or allegation that the privacy rights sought to be afforded by the DPPA have been violated (*e.g.*, the information is ultimately being used to stalk or identify victims of crime or otherwise outside the DPPA permissible uses)—but rather on an improper reading of the statute. Their position can lead only to socially detrimental consequences.

Adoption of Plaintiffs' proposed interpretation of the DPPA would disrupt the balance between privacy and the legitimate governmental and business uses for the information and thwart long-standing practices that serve many segments of society that urgently need access to motor vehicle information for permitted uses. Eliminating information providers from the

process of making data available to legitimate users could drastically hinder certain public safety functions.

Information providers like Defendant-Appellee West Publishing Corporation (“West”) do more than act as a conduit of information. Information providers have applied their knowledge and years of experience to develop tools that allow users to quickly find relevant information from multiple sources, sometimes with less than complete information about the target of the search. Without these tools, for example, law enforcement officials may not be able to quickly obtain accurate identifying information about individuals, and criminal investigations and the eventual apprehension of fugitives could be impeded. If merchants are unable to verify the identify of consumers who present checks or credit cards for payment on the spot, then thieves may have an increased likelihood of successfully accessing and using another individual’s account. Similarly, if potential creditors, landlords or employers are not able to quickly and efficiently verify applicant information, the extension of credit, employment and housing may be delayed or not extended at all.

Because the sensible use of public record information is being challenged, CSPRA and CDIA are vitally interested in the outcome of this appeal. The knowledge and experience of CSPRA and CDIA regarding the information provider industry allow them to provide this Court with an understanding of industry practices and safeguards, as well as the negative impact that will result if this Court reverses the District Court’s Judgment.

Because CSPRA and CDIA have not obtained the consent of all parties to the filing of this amicus brief, they have moved for leave to file this brief.

SUMMARY OF STATEMENT

CSPRA and CDIA urge affirmance of the District Court's decision granting West's motion to dismiss. Many members of CSPRA and CDIA are information providers who obtain in bulk and sell motor vehicle information of the type protected by the DPPA. The information provider industry is a long-established and well-respected industry that obtains, uses and discloses DPPA and similar information for use by legitimate government and business entities. Government and business entities rely on this information to protect and serve individuals throughout the country. Plaintiffs' interpretation of the DPPA would curtail the use of the valuable tools and methods made available by these businesses for practical use of the data.

West's brief explains why—based on settled principles of statutory construction—the district court was correct to conclude that West's obtaining motor vehicle record information for the purpose of reselling it to those with permitted uses does not violate the DPPA. This amicus brief, in turn, discusses (a) the numerous benefits provided by the bulk obtainment and sale of DPPA information; (b) the information provider industry; and (c) the existing security procedures and controls that currently govern the information provider industry's obtainment, use and disclosure of DPPA information.

- I. Governmental Agencies and Private Businesses Rely on Information Providers to Offer Benefits that the States Cannot
- A. Commercial Information Providers Offer Significant Benefits to the Public

Commercial information providers play a vital role in promoting public safety, including various law enforcement efforts, and providing other benefits to the public. Congress did not intend to impair the ability of information providers to offer these benefits. In fact, the DPPA was created as crime prevention legislation. As Senator Harkin, a chief sponsor of the DPPA,

explained, the DPPA “should be interpreted so as not to in any way restrict or hinder law enforcement and crime prevention strategies.”¹

Since the enactment of the DPPA, representatives from the Federal Trade Commission (“FTC”), the Federal Bureau of Investigation (“FBI”), General Accounting Office (“GAO”), and the Department of Homeland Security (“DHS”), as well as state agencies, have spoken about the importance of the services and products provided by information providers to the proper functioning of their agencies. For example, the FTC recognizes that “[b]usiness, government, and private entities use information provided by data brokers for a wide variety of purposes.”² Those purposes include: identity verification and fraud prevention [§ 2721(b)(3)]; insurance claims investigation, antifraud activities and underwriting [§ 2721(b)(6)]; certain statutory compliance efforts [§ 2721(b)(9), (14)]; research activities [§ 2721(b)(5)]; and public safety functions, including tracking and locating individuals linked with terrorism, other criminal suspects and individuals for various purposes (*e.g.*, to distribute an estate, to locate organ donors, or to locate witnesses), enforcing child support orders, and protecting the public health (*e.g.*, locating individuals who have been exposed to harmful and contagious pathogens to reduce the spread of those pathogens) [§ 2721(b)(1), (14)].³

A former FBI director also noted the vital role that information providers play in law enforcement activities. He explained that “[i]nformation obtained is used to support categories of

¹ 139 Cong. Rec. S15962 (Nov. 17, 1993).

² Federal Trade Commission, Prepared Statement before the Senate Committee on the Judiciary, Securing Electronic Personal Data: Striking a Balance Between Privacy and Commercial and Governmental Use at 4 (Apr. 13, 2005), available at <http://www.ftc.gov/os/testimony/050413personaldata.pdf> (last viewed April 6, 2010).

³ *Id.*

FBI investigations, from terrorism to violent crimes, and from health care fraud to organized crime.”⁴ In 1998, the FBI alone made more than 53,000 inquiries to commercial on-line databases.⁵ “[I]nformation from these inquiries assisted in the arrests of 393 fugitives wanted by the FBI, the identification of more than \$37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning.”⁶

The apprehension of the “D.C. Snipers” is an example of the successful use by law enforcement of information databases that contain aggregated motor vehicle records.⁷ The D.C. Snipers killed 10 people and critically injured 3 in Washington D.C., Maryland and Virginia over the course of a month. The FBI and various other state and federal law enforcement agencies used databases containing a variety of information from various states to track down the D.C. Snipers.⁸ Using information generated in a call about an incident in Alabama from someone claiming to be the perpetrator, investigators were able to identify an individual who had previously been arrested in the State of Washington. Those arrest records helped investigators

⁴ Prepared Statement of Louis J. Freeh, Director, FBI before the Senate Appropriations Committee, Commerce, Justice and State, the Judiciary and related Agencies Subcommittee, 1999 WL 170227, at *8 (Mar. 24, 1999).

⁵ CSPRA, Public Benefits from Open Public Records, at 2, available at <http://www.cspra.us/downloads/publicbenefits.pdf>, (last viewed May 7, 2010).

⁶ Prepared Statement of Louis J. Freeh, Director, FBI before the Senate Appropriations Committee, Commerce, Justice, and state, the Judiciary and related Agencies Subcommittee, 1999 WL 170227, at *8 (Mar. 24, 1999).

⁷ Federal Bureau of Investigation, *The Beltway Snipers*, available at <http://www.fbi.gov/page2/oct07/snipers102407.html>, (last viewed May 27, 2010).

⁸ Federal Bureau of Investigation, *The Beltway Snipers*, available at <http://www.fbi.gov/page2/oct07/snipers102207.html>, (last visited May 27, 2010).

identify the name of a second suspect.⁹ Using a database that contained motor vehicle records, authorities were able to identify a New Jersey license plate that was linked to the D.C. Snipers, all within 90 minutes after this information was provided to authorities.¹⁰

More recently, authorities used motor vehicle information to track down the “Time-Square Bomber.” Using the vehicle identification number to track down the owner of a car containing explosive materials that was left abandoned in Times Square, authorities were able to determine that the car was sold in Connecticut. Timing was essential. The suspect was caught while attempting to leave the country. He had been placed on the “do not fly” list, just hours before he was arrested in the airport.¹¹

Data tools provided by commercial information providers also are used to successfully locate abducted children. For example, the National Center for Missing and Exploited Children reports that the United States Marshal Service used commercial information tools to locate a foreign abductor who had smuggled a child into the United States.¹² In another child abduction case,

⁹ Federal Bureau of Investigation, *The Beltway Snipers*, available at <http://www.fbi.gov/page2/oct07/snipers102407.html>, (last viewed May 27, 2010).

¹⁰ Federal Bureau of Investigation, *The Beltway Snipers*, available at <http://www.fbi.gov/page2/oct07/snipers102207.html>, (last visited May 27, 2010).

¹¹ Fox News, May 4, 2010, *Times Square Car Bomb Suspect Faces Terrorism Charges After Admitting to Plot*, available at <http://www.foxnews.com/politics/2010/05/04/times-square-car-bomb-suspect-faces-terrorism-charges-admitting-plot/>, (last viewed May 28, 2010).

¹² National Center for Missing and Exploited Children, *Missing Children Success Stories*, available at www.missingkids/servlet/pageservlet?LanguageCountry=en_US&PageId=3518, (last viewed May 28, 2010).

authorities were able to track down a kidnapper, linked to several child murders, using a partial license plate number.¹³

With respect to child support enforcement, services offered by information providers helped to locate over seventy-five percent of the “deadbeat parents sought.”¹⁴ New York City’s Child Support Enforcement Department used public record information provided by an information provider to recover \$36 million over two years from thousands of non-custodial parents.¹⁵

The states, too, recognize that prohibiting the bulk obtainment and resale of DPPA information would curtail legitimate business and law enforcement interests. In *Taylor v. Axiom Corp.*, the State of Texas, for example, has gone on record as stating:

“Texas itself uses personal driver information compiled and repackaged by private resellers into a convenient format . . . to help track down suspects, witnesses, and other persons of interest, and to achieve other important law enforcement objectives. . . . For example, the Attorney General’s Office routinely uses national databases provided by private resellers to track down individuals who are delinquent in their child-support payments, as well as to help locate suspects in the course of conducting consumer protection and criminal investigations. Plaintiffs’ theory of liability would not just drive these resellers out of business—it would eliminate a valuable tool of law enforcement.”¹⁶

¹³ July 14, 2007, Jennifer Sullivan and Maureen O’Hagon, *Seattle Times*, *Police Seek to Tie Other Cases to Girl’s Death*, available at http://seattletimes.nwsourc.com/html/localnews/2003788864_linnik14m.html, (last viewed May 27, 2010).

¹⁴ CSPRA, Public Benefits from Open Public Records, at 3, available at <http://www.cspra.us/downloads/publicbenefits.pdf>, (last viewed May 7, 2010).

¹⁵ *Id.*

¹⁶ May 8, 2009 *Brief of the State of Texas as Amicus Curiae in Support of Defendants, Taylor v. Acxiom Corp.*, Case No. 08-41083, 41180, 41232, pp. 2-3.

Similarly, during oral argument, Texas stated that “Plaintiffs’ position is actually bad for consumer protection – and bad for law enforcement generally. . . . We need the private sector to help protect consumers and help combat identity fraud. Moreover, we also need the private sector to assist law enforcement.”¹⁷

Not only do government agencies benefit from information providers, but so do consumers. For example, in 1997, eighty-two percent of automobile loan applicants received a loan decision within an hour or less.¹⁸ Similarly, the check verification process for personal checks must occur in a timely fashion. Using the services and tools of an information provider, in just one year, one check verification service was able to verify \$19 billion worth of consumer checks made payable to over 200,000 businesses.¹⁹

The examples could continue, but the above are sufficient to make the point here. Information providers perform important functions that benefit society and further the permissible uses Congress intended to preserve with the DPPA.

B. Information Providers Have Tools Essential to Achieving the above that States Cannot or Do Not Provide

As demonstrated above, the bulk aggregation and resale of public records by information providers result in significant benefits to the public. States cannot or do not provide all of the tools that result in these benefits. Information providers, including members of CSPRA and

¹⁷ *Testimony of James Ho for State of Texas, Taylor v. Acxiom Corp.*, Case Nos. 08-41083, 41180, 41232, (Nov. 4, 2009).

¹⁸ CSPRA, *Consumer Benefits from Public Records*, at 2, available at <http://www.cspra.us/downloads/consumerbenefits.pdf>, (last viewed May 7, 2010).

¹⁹ *Id.*

CDIA, maintain electronic databases of personal information, including motor vehicle records, collected from fifty-three United States jurisdictions. Such databases are essential. Because more than 40 million U.S. residents move each year, to obtain complete information regarding a particular individual, one must search the vehicle records of every state and U.S. territory.²⁰ By combining this information and making it available from one source, an information provider is able to grant access to this information in a cost-effective and timely manner.

While a state might chose to incur the expense and develop such databases itself, Plaintiffs' interpretation would prohibit even this practice as one state does not have its own immediate use to obtain the data from another state. Without access to such databases, a government agency or business would have to conduct individual searches of each separate jurisdiction, a process that would not only waste time and money, but also eliminate many of the time sensitive examples presented above such as tracking down the Times Square Bomber or locating missing children.

The Assistant Director of the FBI's Criminal Division described the tedious process of gathering information without the use of an information provider—something that would result if Plaintiffs' proposed interpretation of the DPPA is adopted. "We would have to physically go down to the courthouse to get real estate records, we would have to be sending these to another state to go get a driver's license record or a picture, we would have to go to a lot of different

²⁰ Personal Information Acquired by the Government from Information Resellers: Is There Need for Improvement?; Joint Hearing before the Subcomm. On Commercial and Administrative Law, Prepared Statement of Stuart K. Pratt, President and CEO of CDIA, 109th Cong. No. 109-08 at 63 (Apr. 4, 2006), available at <http://www.access.gpo.gov/congress/house/pdf/109hrg/26912.pdf>, (last viewed April 6, 2010).

places, and manually gather this information.”²¹ The hours of labor associated with the manual gathering and reviewing of public records each time an enumerated purpose arises carry a significant cost. The tools and services provided by information providers “allow[] FBI investigative personnel to perform searches from computer workstations and eliminate[] the need to perform more time consuming manual searches of federal, state, and local records systems, libraries, and other information sources.”²²

Fortunately, commercial information providers have tools that allow users to access different types of information from different sources using a single query. Commercial information providers also provide tools that allow government agencies and authorities to access information twenty-four hours a day. Without twenty-four hour access, a user might only be able to access public records on business days and during the business hours of a particular records department. Because time is critical in many law-enforcement situations, limited access would not only be inconvenient, but also could substantially impair safety efforts. For example, over half of abducted children who are murdered are killed within three hours of abduction, and almost 99% of abducted children who are murdered are killed within the first 24 hours of abduction.²³

²¹ The Privacy Office, Department of Homeland Security, Privacy and Technology Workshop, Official Transcript at 20 (Sept. 8-9, 2005) (comments of Chris Swecker, Assistant Director of the Criminal Investigative Division for the FBI), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_wkshop_09-2005_transcript_panel1.pdf, (last viewed Apr. 6, 2010).

²² Prepared Statement of Louis J. Freeh, Director, FBI before the Senate Appropriations Committee, Commerce, Justice and State, the Judiciary and Related Agencies Subcommittee, 1999 WL 170227, at *8 (Mar. 24, 1999).

²³ May 2006, Rob McKenna, Attorney General of Washington and U.S. Department of Justice Office of Juvenile Justice and Delinquency Prevention, *Case Management for Missing Children Homicide* (footnote cont'd...)

Moreover, according to a Department of Homeland Security Deputy Director: “[W]e often get more accurate data from the commercial sector. In addition, the processes by which government agencies manage data often makes it difficult to acquire and needs [a] great deal of labor intensity into making it usable and accessible to other entities.”²⁴

For all of these reasons, especially where timing is of the essence, Plaintiffs’ suggestion that it would be a workable solution to limit information providers, as agents, to request an individual’s information from the state only after its user first provides a valid request for personal information (*Plaintiffs’ Brief*, p. 14), would thwart many of the legitimate uses contemplated by the DPPA.

Information providers also offer search tools that allow users to conduct searches using a variety of different search terms and styles. In addition, users are able to conduct searches using incomplete information. For example, a user not knowing whether they were looking for someone with the last name of “Johnson” or “Johndrow” could in one search look for anyone with a last name that started with “John.” Similarly, law enforcement agencies will use commercial information tools to search motor vehicle records using only a partial license plate number, because a witness was unable to recall the complete number. These “wildcard” searches

(...cont'd)

Investigation, p. 13, available at http://www.missingkids.com/en_US/documents/homicide_missing.pdf, (last viewed May 27, 2010).

²⁴ The Privacy Office, Department of Homeland Security, Privacy and Technology Workshop, Official Transcript at 6 (Sept. 8-9, 2005) (comments of Grace Mastalli Principal Deputy Director for the Information Sharing and Collaboration Program at DHS), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_wkshop_09-2005_transcript_panell1.pdf, (last viewed Apr. 6, 2010).

are essential to the efforts of law enforcement and have been developed over the years by the information provider industry.

The tools and services of information providers have resulted in more efficient, accurate and cost-effective verification and location activity. As a result, public safety, law enforcement and consumer protection efforts have become more effective. As Senator Harkin explained, the DPPA should not be interpreted to impair public safety.²⁵ If Plaintiffs' argument is accepted, these benefits will be thwarted, if not eliminated entirely. Such a result would run counter to the purposes of the DPPA and would reduce rather than enhance public safety.

II. The Bulk Obtainment of Motor Vehicle Records by Information Providers Is a Long-Standing and Accepted Practice

Bulk collection of public records and their subsequent resale is a long-standing and common practice that existed prior to the enactment of the DPPA and continues to this day. Prior to the enactment of the DPPA, information providers regularly collected information from various sources, including state departments of motor vehicles ("DMVs"), and sold that information to government agencies and businesses for various legitimate uses. By the time the DPPA was introduced, Congress was aware of the common practice of selling drivers' personal information to entities that would further distribute that information, and Congress did not disturb the practice. Nor did Congress prohibit the practice of obtaining public record information in bulk.²⁶

²⁵ 139 Cong. Rec. S15962 (Nov. 17, 1993).

²⁶ This Court has previously found industry practice relevant to statutory construction. See *Kohl's Food Store, Inc. v. Hyland*, 32 F.3d 1075, 1079 (7th Cir. 1994) (Wisconsin Worker's Compensation Act). *Accord: Yonter v. Aetna Fin. Co.*, 777 F. Supp. 490, 492 (E.D. La. 1991) (considering industry practice in granting summary judgment as to FCRA claims). *S.J. Groves & Sons Co. v. Occupational Safety and Health Review Comm'n*, 648 F.2d 95, 97 (2d Cir. 1981) (Occupational Safety and Health Act of 1970); *Columbia Gas Transmission Corp. v. Fed. Power Comm'n*, 530 F.2d 1056, 1059 (D.C. Cir. 1976) (review of Federal Power Commission certificate order).

As explained by representative Moran, the House Sponsor of the DPPA, the DPPA was designed to continue to permit states to furnish lists of license holder information to various entities, such as information providers.²⁷ As West’s brief explains, the plain text of the DPPA reveals that § 2721(c) does not limit obtainment for resale to only those companies that first use information under § 2721(b).

In the sixteen years since the enactment of the DPPA, DMVs have continued to provide DPPA information in bulk to information providers for resale and nearly every state has enacted its own version of the DPPA. Many government agencies and businesses continue to rely on information obtained by information providers in bulk from state DMVs. The involvement of information providers is well-known and has been since the enactment of the DPPA (including when the statute was amended).

While this point should be readily acknowledged, a review of the public record provides a number of examples:

- The statement of the director of the FBI Louis Freeh before Congress in 1996 regarding the FBI’s reliance on commercial information providers who collect data in bulk and provide invaluable tools for quick and efficient searches of data.²⁸
- The Department of Justice (“DOJ”), the agency charged with enforcing the DPPA, opinion in 1998 that, under the DPPA, state DMVs are permitted to provide bulk data

²⁷ 140 Cong. Rec. H2518 at 2523 (Apr. 20, 1994).

²⁸ Prepared Statement of Louis J. Freeh, Director, FBI before the Senate Appropriations Committee, Commerce, Justice and State, the Judiciary and related Agencies Subcommittee, 1999 WL 170227, at *8 (Mar. 24, 1999).

to commercial information providers who merely intend to resell the information to users with permissible uses.²⁹

In short, the bulk collection and resale of public record information, including motor vehicle information, by information providers who do not intend to make use of the information themselves has been a common and widely-known practice. Both before and after the enactment of the DPPA, Congress was aware of this practice; nevertheless, Congress left in place language in the DPPA to permit this practice.

III. There Are Sufficient Existing Controls to Achieve Balance between Privacy and Accessibility of DPPA Information for Permissible Uses

Plaintiffs' arguments seem to be premised on the mistaken notion that DPPA-regulated information can be adequately protected only if an entity obtaining that information does so one record at a time (that is, not in bulk) and directly from each state. *Plaintiffs' Brief*, p. 14.

However, Plaintiffs' position ignores the explicit protections Congress embedded in the DPPA to ensure that motor vehicle records are put only to permitted uses. For example, the DPPA provides for audits of authorized recipients to ensure that its disclosures were for one of the DPPA's permissible uses.³⁰ Indeed, there are serious consequences if an authorized recipient does not ensure that personal information is disclosed only for the DPPA's permissible uses, especially when an information provider receives that information in bulk. States that fail in their

²⁹ October 9, 1998 letter from R. McFetridge, Special Counsel of the Assistant Attorney General, Civil Division, to P. Sacks, p. 1. West's brief explains the substance of this letter in detail. It is mentioned here only to show that the information provider industry was known and trusted by government agencies.

³⁰ 18 U.S.C. § 2721(c).

duties also must answer to their citizens.³¹ Plaintiffs, therefore, simply are mistaken in their claim that “[a]ny individual could obtain from the state the Personal Information of any number of individuals under the guise of being a ‘reseller’ and, in fact, create a simple website (even overseas beyond the reach of justice) offering to sell that information to people who fill out some forms.” *Plaintiffs’ Brief*, pp. 20-21.

A. Entities that Obtain DPPA Information in Bulk for Resale for DPPA-Permitted Uses Protect that Information from Improper Use

While CSPRA and CDIA advocate for open public record access to ensure that government agencies and businesses have the continued freedom to collect and use public record information, CSPRA and CDIA also promote reasonable security practices to protect that information and to ensure that it is obtained, used and disclosed only by legitimate government and business entities for permissible uses. Best practices require information providers which obtain DPPA information for resale or redisclosure under Section 2721(c) to create and implement policies and procedures to ensure compliance with the DPPA. These requirements typically include (1) the establishment of a chief information officer or chief information security officer to manage the information security practices surrounding the handling of DPPA information, (2) the provision of training for employees and customers in the proper use of DPPA information, (3) credentialing of customers to limit access to persons with permitted uses, (4) the implementation of contractual provisions requiring customers to certify the permissible uses for which they will

³¹ State officials who violate the DPPA may find themselves defending both a DPPA and a civil rights action. 18 U.S.C. § 2723(b) (“Any state department of motor vehicles that has a policy or practice of substantial noncompliance with this chapter shall be subject to a civil penalty imposed by the Attorney General of not more than \$5,000 a day for each day of substantial noncompliance.”). See also, *Collier v. Dickinson*, 477 F.3d 1306, 1311 (11th Cir. 2007), *cert. denied*, 552 U.S. 1096, 128 S. Ct. 869 (U.S. 2008) (ruling that rights protected by the DPPA are enforceable under 42 U.S.C. § 1983).

use the information, and (5) obligating customers to provide adequate security surrounding the handling of the information.

For example, it is standard practice for information providers to sell personal information only to legitimate businesses or organizations that have certified compliance with the various statutory schemes, including the DPPA.³² Prior to receiving that information from the vendors, those businesses and organizations undergo certain vetting processes and are subject to oversight by the vendors to ensure that their handling of the personal information complies with all federal and state laws.³³ Thus, Plaintiffs' DPPA information obtained by information providers such as West will be adequately protected by these procedures.

The DPPA itself ensures that an entity (such as West) obtaining DPPA information will disclose that information only for one of the DPPA's fourteen permissible uses.³⁴ An information provider disclosing this information other than for one of these permissible uses may be held liable to the individual to whom the information pertains for actual damages or liquidated damages of at least \$2,500, and, for willful violations, punitive damages and attorney's fees.³⁵ The price to obtain a report on an individual containing public record information is generally just a few dollars, in some cases just a few cents. Given the difference in price versus potential exposure, information providers have an economic incentive to put in place procedures to assure that DPPA information is used only for permissible uses.

³² Lynn Peterson and Genie Tyburski, *The Truth about Big Brother Databases* (Oct. 3, 2002), available at www.cspra.us/downloads/BigBrotherDatabases.htm, (last viewed May 3, 2010).

³³ *Id.*

³⁴ 18 U.S.C. § 2721(c).

³⁵ 18 U.S.C. § 2724.

B. For Some Information Providers, the GLBA Safeguards Rule Further Protects DPPA Information

Some information providers are subject to the Safeguards Rule mandated by the Gramm-Leach-Bliley Act.³⁶ The Safeguards Rule is designed to protect the security and confidentiality of certain information and to protect that information against anticipated threats, hazards or unauthorized access.³⁷ An information provider subject to the Safeguards Rule must develop and maintain a comprehensive information security program containing administrative, technical and physical safeguards for the information.³⁸ The security program must contain a risk assessment to identify foreseeable internal and external risks to the security, confidentiality and integrity of the information, and must provide safeguards to control those risks.³⁹ The Federal Trade Commission is authorized to investigate and enforce the Safeguards Rule.

As a result, DPPA information is adequately protected even if information providers are permitted to obtain that information in bulk as authorized recipients under 18 U.S.C. § 2721(c).

IV. Conclusion

For the above reasons, this Court should affirm the District Court's judgment granting West's motion to dismiss.

³⁶ Federal Trade Commission, Final Rule, Standards for Safeguarding Customer Information, 67 Fed. Reg. 36484-485 (May 23, 2002).

³⁷ 16 C.F.R. § 314.3(b).

³⁸ 16 C.F.R. § 314.3(a).

³⁹ 16 C.F.R. § 314.3(b).

Dated: June 23, 2010

Amicus Curiae the Coalition for Sensible
Public Records Access and the Consumer Data
Industry Association

By: _____

Ronald I. Raether, Jr. (Ohio Bar 0067731)
Faruki Ireland & Cox P.L.L.
500 Courthouse Plaza, S.W.
Dayton, Ohio 45402
(937) 227-3700

Attorneys for Amicus Curiae

Certificate of Compliance

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because:

X this brief contains _____ words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii), or

___ this brief uses a monospaced typeface and contains [state the number of] lines of text, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(A)(5) and Circuit Rule 32, and the type style requirements of Fed. R. App. P. 32(a)(6) because:

X this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2002 in size 12 font with Times New Roman type style for all headings and text, or

___ this brief has been prepared in a monospaced typeface using [state name and version of word processing program] with [state number of characters per inch and name of type style].

Dated: June 23, 2010

Attorneys for Amicus Curiae

PROOF OF SERVICE

The undersigned certifies that on June 23, 2010, I had hand-delivered fifteen copies of the Brief of Amicus Curiae to the Clerk of Court, United States Court of Appeals for the Seventh Circuit, and I mailed via Federal Express two copies of the Brief of Amicus Curiae to counsel for Plaintiffs and West Publishing.

Attorneys for Amicus Curiae

393775.1