IN THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF FLORIDA TALLAHASSEE DIVISION

MICHAEL WELCH,

Plaintiff,

v. CASE NO. 4:09cv302-RH/WCS

JULIE L. JONES in her official capacity as executive director of the Florida Department of Highway Safety and Motor Vehicles,

Defendant.

_____/

ORDER ON THE MERITS

The Driver's Privacy Protection Act ("DPPA") prohibits a state from disclosing "personal information" from its driver's license records but allows the state to disclose the information "for use" in one of 14 specified ways. *See* 18 U.S.C. § 2721(a) & (b). The State of Florida discloses personal information from its driver's license records in bulk to a for-profit corporation that, through a related entity, makes the information available over the internet to any user who provides the user's identity, pays a fee, and swears under penalty of perjury that the information will be used in one of the 14 specified ways. Aside from the common

knowledge that some people lie, there is no evidence that the state's disclosure of the information has resulted or is likely to result in the use of the information other than in the 14 specified ways. I conclude that under these circumstances, the state has disclosed the information "for use" only in the 14 specified ways and thus has not violated the DPPA. This order sets out the court's findings of fact and conclusions of law following a bench trial.

I

ShadowSoft, Inc. ("ShadowSoft") is a for-profit corporation based in Dallas, Texas. It maintains a website—publicdata.com—and provides other services for The Source for Public Data ("Public Data"). Public Data is a for-profit partnership organized under Texas law. Bruce Stringfellow is the sole shareholder and president of ShadowSoft and is the sole shareholder and president of a separate corporation that is the general partner of Public Data. Mr. Stringfellow is a limited partner of Public Data.

Public Data's business is selling information obtained from governmental sources—federal and state agencies of various kinds—to customers who subscribe to Public Data's service on a monthly or annual basis. A customer cannot subscribe anonymously; instead, the customer must pay with a credit card and must provide the customer's name and other identifying information, including—for individuals—the customer's driver's license number. Public Data verifies the

information, including by matching the credit-card billing address and matching the driver's license information if the customer is from a state for which Public Data has driver's license information. The number of states for which Public Data has driver's license information has been higher but is down to three, including Florida.

ShadowSoft began buying Florida driver's license information from the state in 1999. It entered formal contracts governing the purchases in 2006 and 2009. The 2009 contract—denominated a "memorandum of understanding"—is in effect at this time. The contract discloses that ShadowSoft will provide the purchased information to Public Data and that Public Data will do two things with it: first, use the information to verify the identity of Public Data's own customers; and second, make the information available to Public Data's customers. There is no evidence that ShadowSoft has ever misled the State about its intended use—or Public Data's intended use—of the information.

Public Data uses the information precisely as ShadowSoft said it would. Public Data uses the information to verify the identity of Florida customers attempting to subscribe to Public Data's services. And it makes the information available to subscribers. Before a subscriber can obtain Florida driver's license information, however, the subscriber must identify the subscriber's intended use of the information—from a drop-down menu listing the 14 specified ways in which

the information can properly be used under the DPPA. The subscriber must swear under penalty of perjury that the specified exemption—the use selected from the drop-down menu—applies. The website conspicuously warns that unauthorized use of the data may result in penalties under state and federal law.

The named plaintiff Michael Welch is a licensed Florida driver. His driver's license information was sold to ShadowSoft and in turn made available over the Public Data website. But nobody—except his own lawyer in connection with this lawsuit—has ever accessed his information.

II

Mr. Welch represents a class—certified under Federal Rule of Civil Procedure 23(b)(2)—consisting of each individual with a Florida driver's license whose "personal information," as defined in the DPPA, has been disclosed to ShadowSoft or Public Data since September 30, 2004. Though Mr. Welch earlier named additional defendants and sought an award of damages as well as declaratory and injunctive relief, he now names a single defendant—the executive director of the Florida Department of Highway Safety and Motor Vehicles in her official capacity—and seeks only declaratory and injunctive relief. For convenience, this order sometimes refers to the defendant's assertions as those of the "State."

III

Mr. Welch's claim is that the State's disclosure of driver's license information to ShadowSoft violates the DPPA. The State's first defense is that Mr. Welch has suffered no injury in fact because nobody—other than his own lawyer—has accessed the information or is likely to do so. But that misses the point. The information was disclosed *to ShadowSoft.* Mr. Welch says he has suffered and is continuing to suffer injury in fact because of the disclosure to ShadowSoft, especially in light of the further availability of the information over the internet to anyone willing to claim a permissible purpose for accessing it. When personal information is disclosed in violation of the DPPA—as Mr. Welch says happened when the State disclosed his information to ShadowSoft—the DPPA explicitly creates a private right of action in favor of "the individual to whom the information pertains." 18 U.S.C. § 2724(a). In this instance that means Mr. Welch and also every class member. And having one's personal information disclosed and available for further disclosure—in the first instance to a single corporation such as ShadowSoft and then through a website even if nobody has yet accessed it—is a sufficient injury in fact to confer constitutional standing. Mr. Welch's ability to recover—and the class's—turns not on standing or the extent of any injury but on whether the DPPA has been and is being violated.

IV

The DPPA provides different levels of protection for "personal information" and "highly restricted personal information." At issue in this case is only "personal information." "Personal information" means

> information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status.

18 U.S.C. § 2725(3).

In § 2721(a), the DPPA prohibits a state department of motor vehicles or its representative from disclosing "personal information" from driver records "except as provided in subsection (b) of this section"—that is, except as provided in § 2721(b). Similarly, in § 2722(a), the DPPA makes it "unlawful" for *any* person—not just a state employee—to "obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b)." A knowing violation of the DPPA is an offense punishable by a fine. *Id.* § 2723(a).

Thus under the plain terms of the statute, the State's disclosure of personal information to ShadowSoft was lawful if and only if authorized under § 2721(b). That subsection requires a state to disclose information for specific vehicle-related purposes—for example, in connection with thefts or recalls—and allows a state to disclose personal information on 14 other grounds:

(1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.

(2) For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts and dealers; motor vehicle market research activities, including survey research; and removal of non-owner records from the original owner records of motor vehicle manufacturers.

(3) For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only--

> (A) to verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and
>
> (B) if such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.

(4) For use in connection with any civil, criminal, administrative, or arbitral proceeding in any Federal, State, or local court or agency or before any self-regulatory body, 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.

(5) For use in research activities, and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.

(6) For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in

> connection with claims investigation activities, antifraud activities, rating or underwriting.
>
> (7) For use in providing notice to the owners of towed or impounded vehicles.
>
> (8) For use by any licensed private investigative agency or licensed security service for any purpose permitted under this subsection.
>
> (9) For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under chapter 313 of title 49.
>
> (10) For use in connection with the operation of private toll transportation facilities.
>
> (11) For any other use in response to requests for individual motor vehicle records if the State has obtained the express consent of the person to whom such personal information pertains.
>
> (12) For bulk distribution for surveys, marketing or solicitations if the State has obtained the express consent of the person to whom such personal information pertains.
>
> (13) For use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.
>
> (14) For any other use specifically authorized under the law of the State that holds the record, if such use is related to the operation of a motor vehicle or public safety.

18 U.S.C. § 2721(b).

V

Before turning to an analysis of whether the State's disclosure of information to ShadowSoft fits within the § 2721(b) exceptions, a word is in order

about the statute's next provision, § 2721(c):

> Resale or redisclosure.—An authorized recipient of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information only for a use permitted under subsection (b) (but not for uses under subsection (b) (11) or (12)). An authorized recipient under subsection (b)(11) may resell or redisclose personal information for any purpose. An authorized recipient under subsection (b)(12) may resell or redisclose personal information pursuant to subsection (b)(12). Any authorized recipient (except a recipient under subsection (b) (11)) that resells or rediscloses personal information covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request.

The State says that § 2721(c) creates an additional exception to the ban on the disclosure of personal information, separate and apart from the exceptions set out in § 2721(b). That is not so. Under § 2722(a), it is "unlawful . . . to obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b)." Period. This provision is flatly inconsistent with the assertion that there is an additional exception under § 2721(c) for information that does not fit within a § 2721(b) exception.

Two other provisions further confirm this analysis. First, § 2721(a) prohibits a state department of motor vehicles or its representative from disclosing personal information from driver records except as provided in § 2721(b)—not also as provided also in § 2721(c). Second, § 2721(d) allows a state to establish

procedures under which, when a request for information is received that does not come within a § 2721(b) exception, the state may ask the driver to consent to the disclosure and tell the driver that if the driver does not consent, the information will not be released; the section does not allow the state to tell the driver that if the driver does not consent, the information may nonetheless be disclosed under § 2721(c).

In short, the statute makes clear time and again that the only permitted disclosures are those set out in § 2721(b). An "authorized recipient" of personal information within the meaning of § 2721(c) is a person authorized to receive the information based on the § 2721(b) exceptions. The plain language of the statute makes this clear.

VI

The issue, then, is simply whether the State's disclosure of information to ShadowSoft fits within the § 2721(b) exceptions, that is, whether the State discloses the information "for use" in one of the 14 ways permitted under § 2721(b).

ShadowSoft makes the information available to Public Data, which does two things with the information. First, the information is used to verify the identity of Public Data's Florida subscribers. Second, the information is made available to Public Data subscribers who swear under penalty of perjury that they are obtaining

the information for use in one of the 14 ways permitted by § 2721(b). Public Data's two uses of the information raise distinct issues.

A

Public Data's use of the information to verify the identity of its subscribers fits easily within § 2721(b)(3). That subsection allows the disclosure of personal information from driver's license records "[f]or use in the normal course of business by a legitimate business . . . to verify the accuracy of personal information submitted by" the driver to the business. Public Data is a legitimate business, and its use of information to verify its subscribers' identities is precisely the use permitted by the statute.

Mr. Welch says, though, that § 2721(b)(3) allows a state to disclose only the personal information of a business's actual customer at the time of an actual transaction. Mr. Welch says the provision does not allow the state to turn over to a business in advance the personal information of every driver in the state—including individuals who will never have any contact with the business. One could plausibly so read the statute.

The better view, though, is that when a business obtains personal information in advance for the very purpose of having the information available to verify a customer's identity when the need arises, the information is obtained "for use" in verifying the customer's identity. A person buys an umbrella for use in the

rain, even if the person is fortunate enough never to actually use it. A homeowner buys a fire extinguisher for use in a fire, even if there is no fire. And as one court has noted, a lawyer or judge buys the entire set of the Federal Reporter for use in legal research, even if some volumes are never opened. *See Taylor v. Acxiom Corp.*, 612 F.3d 325, 337 (5th Cir. 2010). Had Congress intended § 2721(b) to require actual use—rather than only a purpose to use when appropriate—it could have said so. And had Congress intended information to be disclosed only for an individual transaction, rather than in bulk, it could have said that, too. But it did not. *See Taylor*, 612 F.3d at 335-37 (further analyzing the statute's language and legislative history, applying canons of construction, and concluding that the permitted uses under § 2721(b) generally apply to bulk as well as individual disclosures).

Mr. Welch says, though, that under this reading the statute can easily be evaded by any business willing to falsely claim it will use the information in this way—that is, by any business that is willing to subject itself to the substantial civil and criminal penalties for obtaining information improperly and that has an agent willing to risk a prosecution for perjury. The argument is more hypothetical than real. This record provides no support for the proposition than any business would be willing to spend the substantial sum necessary to buy these records without an actual and obvious purpose for doing so. The record provides no support for the

proposition that the State would be willing to sell the records on a pretext. And in any event, if the statute as written allows evasion, the remedy is for Congress to amend the statute, not for a court to do so under the guise of construction.

In sum, the statute allows a state to disclose information in bulk on all its drivers to a business whose purpose in obtaining the information is to verify its customers' identities.

B

This is not, though, ShadowSoft's only purpose for obtaining the records. The more important purpose is to make the records available to Public Data and in turn to Public Data's subscribers. Indeed, if it were not for the intent to make the information available to Public Data's subscribers, ShadowSoft almost surely would not buy the information at all. A person who obtains personal information for a permitted use—such as verifying customer identity—is not free to use or disclose the information for a different, unauthorized purpose. *See* 18 U.S.C. § 2721(c). So ShadowSoft's acquisition of the records is proper only if—separate and apart from Public Data's use of the records to verify its customers' identities—the acquisition of the records fits within the § 2721(b) exceptions.

The relevant facts are straightforward: the State discloses personal information to ShadowSoft, which makes it available through Public Data's website to Public Data subscribers who identify themselves and swear under

penalty of perjury that they are obtaining the information for use in one of the 14 ways permitted under § 2721(b). The question is whether, under these circumstances and without regard to Public Data's use of the information to verify its customers' identities, the State's disclosure of information to ShadowSoft is "for use" in one of the 14 permitted ways.

On one view, the answer is no, because neither ShadowSoft nor Public Data uses the information in one of the 14 ways. Public Data uses the information, instead, as stock in trade, much as a grocer uses a tomato. But on a more comfortable reading of the language, the answer is yes. The State discloses the information to ShadowSoft and in turn to Public Data "for use" in one of the 14 permitted ways, just as a farmer grows a tomato for human consumption, even if the farmer sells it to a grocer for whom it is stock in trade. Especially in a statute imposing civil penalties and fines, this is the better reading of "for use."

This result is fully consistent with the only circuit decision that touches on the issue. *See Taylor v. Acxiom Corp.*, 612 F.3d 325, 338-39 (5th Cir. 2010)). And the result is fully consistent with the majority view in the district courts. *See Wiles v. ASCOM Transp. Sys., Inc.*, Civ. No. 3:10-CV-28-H, 2010 WL 5055698 (W.D. Ky. Dec. 3, 2010); *Cook v. ACS State & Local Solutions, Inc.*, ___ F. Supp. 2d ___, 2010 WL 4813848 (W.D. Mo. Nov. 19, 2010); *Young v. West Publ'g Corp.*, 724 F. Supp. 2d 1268 (S.D. Fla. 2010); *Graczyk v. West Publ'g Corp.*, No.

09 C 4760, 2009 WL 5210846 (N.D. Ill. Dec. 23, 2009); *Russell v. ChoicePoint Servs., Inc.*, 300 F. Supp. 2d 450 (E.D. La. 2004). *But see Roberts v. Source for Public Data*, No. 08-4167-CV-C-NKL, 2008 WL 5234675 (W.D. Mo. Dec. 12, 2008); *Locate.Plus.Com, Inc. v. Iowa Dep't of Transp.*, 650 N.W.2d 609 (Iowa 2002).

Mr. Welch says, though, that on this reading the statute will not accomplish the congressional objectives of protecting privacy and avoiding the misuse of personal information from driver's license records. In one respect he is right; the statute will not ensure that personal information is never improperly disclosed or used. But it is difficult to conceive a statute that *would* ensure that result. And in any event Mr. Welch is wrong to assert that on this reading the statute accomplishes nothing. Public Data discloses information only to a user who provides an identity that Public Data takes reasonable steps to verify. Public Data discloses information only to a user who swears under penalty of perjury that the information will be used for a permitted purpose. Public Data conspicuously warns users that misuse violates state and federal law. And Public Data keeps a record of everyone who accesses the information. These steps do not render misuse impossible, but they undoubtedly have at least some effect in reducing the misuse of personal information from driver's license records. Indeed, a member of Congress might reasonably conclude that a person bent on misusing personal

information would find an easier way to get it than jumping through the Public Data hoops and risking a perjury prosecution. And in any event, if these steps are insufficient, the remedy lies with Congress or the state legislature.

VII

The State discloses information to ShadowSoft and in turn to Public Data "for use" in the 14 ways permitted under 18 U.S.C. § 2721(b). Accordingly,

IT IS ORDERED:

The clerk must enter a judgment stating:

> It is declared that the disclosure of "personal information" from driver's license records by the State of Florida Department of Highway Safety and Motor Vehicles to ShadowSoft, Inc., in accordance with the 2009 memorandum of understanding between them does not violate the Driver's Privacy Protection Act. All further claims in this action are dismissed with prejudice.

SO ORDERED on March 3, 2011.

s/Robert L. Hinkle
United States District Judge