

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF INDIANA
SOUTH BEND DIVISION

RACHEL A. WHITAKER AND)	
RICHARD L. DUNKIN,)	
)	
Plaintiffs,)	
)	
v.)	Cause No. 3:13-cv-826 RLM-CAN
)	
APPRISS, INC.,)	
)	
Defendant.)	

OPINION AND ORDER

The Driver’s Privacy Protection Act of 1994, 18 U.S.C. § 2721 *et seq.*, secures from prying eyes the personal information held in state department of motor vehicles records. Appriss, Inc. sold two drivers’ accident reports to businesses, which then used those reports to solicit the drivers. The drivers brought a putative class action against Appriss for violating the DPPA, and Appriss now moves for summary judgment.

I. BACKGROUND

The Indiana State Police contracted with Appriss to design and to maintain the Automated Reporting Information Exchange System, or ARIES. ARIES offered a uniform accident report for police throughout the state, a software platform for police to complete accident reports, and electronic storage for completed accident reports.

Police officers had two options when filling drivers’ personal information into the Indiana Officer’s Standard Crash Report. They could manually type in

the driver's contact and vehicle information. Or they could use a handheld scanner to scan the barcodes on the back of the driver's license and registration documents. Once the scanner read the barcode, it would auto-populate the accident report with the information listed on the driver's license and registration, including the driver's name, address, and license number. The only practical difference between these methods was that using the scanner would save time for officers and avoid typographical errors.

The barcode method never accessed the Bureau of Motor Vehicles' own database of driver data. It used no internet connection at all. The driver's license barcode was encoded with the information on the front of the driver's license – the scanner simply read it and input the information into the form.¹ Once an officer completed the crash report, often after filling in details about the accident back at the station, the report would then upload to the ARIES database.

Appriss made completed crash reports available on its website, www.buycrash.com. The state police required ARIES to be a “self-funded” program, meaning that Appriss relied on user fees from the website to make money, without charging the state for its services. Through the website, Appriss allowed parties involved in accidents to purchase copies of their accident reports. Appriss also allowed the general public, including businesses, to buy individual reports or to pay a subscription fee that allowed them to access reports in bulk. Companies that purchased accident reports could then use them to solicit

¹ Appriss had a third method to populate the accident reports that involved logging into the BMV database. This method wasn't available to either police department involved in this litigation.

clients. According to Appriss's contract, the state police authorized the specific fees that Appriss charged to the public, and Appriss remitted a portion of the fees paid to it back to the state police. ARIES would also send all new and updated crash report data to the BMV every day, allowing the BMV to investigate financial responsibility in accidents and to suspend licenses as needed.

The BMV stores all of its driver, vehicle, and title records in the STARS (System Tracking and Record Support) system. Police officers can use the Indiana Data and Communications System, or IDACS, to access the records in STARS to check the validity of drivers' licenses. The BMV logs every IDACS request to access STARS, including the date and information accessed. IDACS seems to be the only way for an officer to access STARS data.

The plaintiffs argue that Appriss impermissibly disclosed their contact information, contained in their accident reports, to third-party businesses that then used that information to solicit them without their consent.

The first plaintiff is Rachel Whitaker, who was in a car accident in Kokomo, Indiana. Officer Cunningham responded to the accident. He initially didn't want to prepare an accident report because he believed that the damage to her car was worth less than \$1,000. Ms. Whitaker insisted that he complete one anyway. She says she gave Officer Cunningham her driver's license and registration, and Officer Cunningham then returned to his car with these items.

Officer Cunningham explained that, when responding to accidents, he often uses IDACS to check the validity of a driver's license. He said that he then takes handwritten notes on a blank Standard Crash Report form, seemingly

without using the auto-populate feature from the barcode scanner. When he gets back to the station, he uses his notes to create an electronic version of the accident report for ARIES. Officer Cunningham says he would have followed these steps when he responded to Ms. Whitaker's accident. According to a BMV representative, Ms. Whitaker's information wasn't accessed through IDACS on the date of the accident. Her accident report was uploaded to ARIES on the day of her accident. The report was updated at a later date, but only to include data on the accident's location.

About a month after the accident, Ms. Whitaker received letters from a personal injury law firm and from a chiropractor advertising their services and indicating knowledge that she had recently been in a car accident. According to Appriss, five different entities purchased Ms. Whitaker's accident report.

The second plaintiff is Richard Dunkin, who was involved in an accident in Carrol County, Indiana. Deputy Schimmel responded to the accident. Mr. Dunkin says he gave his driver's license, vehicle registration, and proof of insurance to Deputy Schimmel, who then took them back to his police car.

Deputy Schimmel's usual practice when responding to an accident is to ask the driver for his license, registration, and insurance documents. He would scan the barcodes on the license and registration to auto-populate the accident report form.

Deputy Schimmel also generally calls the dispatcher to request a "10/27," code for a confirmation that a driver's license is valid and that the holder has no outstanding warrants. In calling for a 10/27, he usually provides a combination

of the driver's name, birth date, or license number. The dispatcher then uses IDACS to access the BMV's STARS database to check whether the license is valid. When dispatch checks on a license, it usually relays some information, such as the driver's name and address, back to the police officer. Deputy Schimmel says he probably wouldn't compare that information against what was written on the license, and he's usually just concerned with whether the license is valid. BMV records show that there was a STARS information request, through IDACS, for Mr. Dunkin on the date of his accident. Mr. Dunkin's accident report was uploaded to ARIES and no changes were ever made to it.

About a month after the accident, Mr. Dunkin received solicitations from businesses with which he had no relationship, and which indicated their knowledge that he had recently been in a car accident. According to Appriss, six different entities purchased Mr. Dunkin's accident report.

The plaintiffs weren't the victims of stalking or identity theft from the disclosure of their personal information. Neither suffered any monetary loss or physical harm from the disclosure. Ms. Whitaker said she "resented," and Mr. Dunkin said it was "scary," that strangers could obtain their information so readily.

Ms. Whitaker and Mr. Dunkin claim that Appriss violated the Driver's Privacy Protection Act when it sold copies of accident reports containing personal information to third parties for solicitation purposes and without their consent. The plaintiffs seek liquidated damages in the amount of \$2,500 each, § 2724(b)(1), and class certification, Fed. R. Civ. P. 23.

The court denied Appriss's motion to dismiss for failure to state a claim. Whitaker v. Appriss, Inc., No. 3:13-cv-826, 2014 WL 4536559 (N.D. Ind. Sept. 11, 2014). The court bifurcated discovery, delaying any ruling about the potential class action until the court determines whether the named plaintiffs prevail. In 2016, the Supreme Court decided *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), which provided guidance on Article III standing. Based on *Spokeo*, Appriss moved to dismiss for lack of jurisdiction. Fed. R. Civ. P. 12(b)(1). The court decided that the plaintiffs have standing and the case continued through discovery. Whitaker v. Appriss, Inc., 3:13-cv-826, 2017 WL 193056 (N.D. Ind. Jan. 17, 2017). Appriss now moves for summary judgment. Fed. R. Civ. P. 56.

II. STANDARD OF REVIEW

Summary judgment is appropriate when the pleadings, discovery materials, disclosures, and affidavits demonstrate no genuine issue of material fact, such that the movant is entitled to judgment as a matter of law. Fed. R. Civ. P. 56; Protective Life Ins. Co. v. Hansen, 632 F.3d 388, 391-392 (7th Cir. 2011). The evidence and all inferences that reasonably can be drawn from it must be construed in the light most favorable to the non-moving parties. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 255 (1986). As the moving party, Appriss bears the burden of informing the court of the basis for its motion, together with evidence demonstrating the absence of any genuine issue of material fact. Celotex Corp. v. Catrett, 477 U.S. 317, 323 (1986). If Appriss meets that burden, the plaintiffs can't rest upon the allegations in the pleadings, but must "point to

evidence that can be put in admissible form at trial, and that, if believed by the fact-finder, could support judgment in [their] favor.” Marr v. Bank of Am., N.A., 662 F.3d 963, 966 (7th Cir. 2011); Hammel v. Eau Galle Cheese Factory, 407 F.3d 852, 859 (7th Cir. 2005) (summary judgment is “not a dress rehearsal or practice run; it is the put up or shut up moment in a lawsuit, when a party must show what evidence it has that would convince a trier of fact to accept its version of events”).

III. DISCUSSION

Congress enacted the DPPA to prevent “stalkers and criminals from utilizing motor vehicle records to acquire information about their victims,” and to stop “the States’ common practice of selling personal information to businesses engaged in direct marketing and solicitation.” Dahlstrom v. Sun-Times Media, LLC, 777 F.3d 937, 944 (7th Cir. 2015) (quoting Maracich v. Spears, 133 S. Ct. 2191, 2198 (2013)). The Act prohibits state departments of motor vehicles from “knowingly disclos[ing] or otherwise mak[ing] available to any person or entity . . . personal information . . . about any individual obtained by the department in connection with a motor vehicle record,” except as allowed under the statute’s fourteen exceptions. 18 U.S.C. § 2721(a)(1). The Act prohibits “any person [from] knowingly [] obtain[ing] or disclos[ing] personal information, from a motor vehicle record, for any use not permitted under” one of the exceptions. § 2722(a). A “motor vehicle record” is “any record that pertains to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration, or

identification card issued by a department of motor vehicles.” § 2725(1). The Act confers a private right of action on people whose information was wrongfully obtained or disclosed for, among other things, “actual damages, but not less than liquidated damages in the amount of \$2,500.” § 2724(a), (b)(1).

The court holds that name, address, and driver’s license number written down or scanned from a driver’s license handed over by the license-holder isn’t “personal information, from a motor vehicle record,” protected by the DPPA. § 2722(a). Appriss didn’t violate the DPPA when it sold the plaintiffs’ personal information to businesses to solicit them.

A. The law of the case

Appriss first argues that the court’s earlier opinions compel judgment in its favor. See United States v. Thomas, 11 F.3d 732, 736 (7th Cir. 1993) (“[W]hen a court decides upon a rule of law, that decision should continue to govern the same issues in subsequent stages of the same case.”).

In ruling against Appriss’s motion to dismiss, the court looked to *Senne v. Village of Palatine*, 695 F.3d 597 (7th Cir. 2012), which held that personal information printed onto a parking ticket is “personal information . . . about any individual obtained by the department in connection with a motor vehicle record,” 18 U.S.C. § 2721(a), and thus falls within the DPPA’s scope. Senne v. Vill. of Palatine, 695 F.3d 597, 601-603 (7th Cir. 2012). *Senne* wasn’t a case in which the plaintiff herself disclosed the information, but where the police officer accessed the DMV database to prepare the ticket. It led to this court’s conclusion

that “[i]f the original source of the other government agency’s information is the state department of motor vehicles, the DPPA protects the information throughout its travels.” Whitaker v. Appriss, Inc., No. 3:13-cv-826, 2014 WL 4536559, at *4 (N.D. Ind. Sept. 11, 2014) (citing Senne, 695 F.3d at 609).

An accident report itself isn’t a motor vehicle record, but “disclosure of personal information that was obtained by and from the department of motor vehicles may nonetheless violate the DPPA.” *Id.* at *5 (discussing Mattivi v. Russell, No. Civ.A. 01-WM-533(BNB), 2002 WL 31949898 (D. Colo. Aug. 2, 2002)). The decisive factor is “how the police officer who created the accident report obtained the driver’s license and vehicle title information – from the plaintiffs themselves or from the state department of motor vehicles.” *Id.*; see Pavone v. Meyerkord & Meyerkord, LLC, 118 F. Supp. 3d 1046, 1054 (N.D. Ill. 2015) (“To the extent that the Schaumburg Police Department received the Pavones’ personal information verbally from the Pavones—a reasonable inference given they were at the scene of the accident—this would not constitute a violation of the DPPA.”).

But the earlier opinion isn’t explicit as to whether personal information pulled from a driver’s license, without accessing the BMV’s database, is information “from the plaintiffs themselves[, who handed over their driver’s licenses,] or from the state department of motor vehicles[, which created the licenses using its records of the drivers’ personal information].” *Id.* The “original source” can be characterized either way. The law of the case doesn’t provide Appriss with a clear route to victory.

B. The statute

The first issue is whether the driver's license itself is a "motor vehicle record." If so, the disclosure of personal information from it would fall under the statute. A "motor vehicle record" is "any record that *pertains to* a motor vehicle operator's permit . . . or identification card issued by a department of motor vehicles." 18 U.S.C. § 2725(1) (emphasis added). The word "pertains," as used in the DPPA, means "to belong as a part, member, accessory, or product." Lake v. Neal, 585 F.3d 1059, 1061 (7th Cir. 2009). A driver's license isn't a part, member, accessory, or product of a motor vehicle operator's permit; it *is* a motor vehicle operator's permit. The plaintiffs suggest that "pertains" is intentionally expansive. As explained later, such an expansive reading would pull conduct into the Act's orbit well beyond what Congress intended to govern. The license itself isn't the relevant "motor vehicle record."

If there's a possible claim, the relevant record would have to be that on which each license was based and which contains the driver's personal information. This record would "belong as a part" to the driver's license, without contorting the word "pertain." If the "original source" of the information on the license is the BMV, then the information falls under the Act's scope. Whitaker v. Appriss, Inc., No. 3:13-cv-826, 2014 WL 4536559, at *4 (N.D. Ind. Sept. 11, 2014) (citing Senne v. Vill. of Palatine, 695 F.3d 597, 609 (7th Cir. 2013)). The only issue then is whether the "original source" of the information is the DMV or the plaintiffs.

Other courts interpret DPPA protection to require that the information in a record be disclosed by a DMV, and not the plaintiff. The Second Circuit adopted this interpretation in *Fontanez v. Skepple*, 563 F. App'x 847 (2d Cir. 2014). The plaintiff in that case produced her driver's license as identification at a jail so that she could visit her incarcerated boyfriend. The defendant, a corrections officer, used the address from her license to send her a teddy bear and note describing himself as her "new admirer." *Id.* at 848. The Second Circuit held that "[w]here the personal information at issue is not obtained from a state DMV, no DPPA cause of action can be found." *Id.* at 849. "[T]he DPPA does not protect against the use of personal information obtained from a driver's license provided by the holder as proof of identity to gain access to a facility." *Id.* at 848. The "access to a facility" language arguably limits the reach of the court's holding, but nothing in the statute suggests that DPPA scope is related to whether the holder uses a license to gain access to a facility or for any other purpose. Because the plaintiff provided the license containing the information, there's no DPPA claim when that information is misused.

The Eleventh Circuit's interpretation accords with the Second Circuit's. In *Siegler v. Best Buy Co. of Minnesota*, 519 F. App'x 604 (11th Cir. 2013), a customer returned a computer mouse to Best Buy. To complete the return, the cashier took the customer's driver's license and scanned the magnetic strip on it. *Id.* at 604. The customer demanded that the information from the license be deleted and, when Best Buy didn't do so, he sued for violating the DPPA. *Id.*

The court held that “the Act is concerned only with information disclosed, in the first instance, by state DMVs.” *Id.* at 605. “[T]he Act was intended to prohibit only the disclosure or redisclosure of information *originating* from state department of motor vehicles . . . records.” *Id.* (emphasis in original). That the plaintiff disclosed the information removed it from the scope of the act. *See also* Hurst v. State Farm Mut. Auto. Ins. Co., No. 10-1001-GMS, 2012 WL 426018, at *10 (D. Del. Feb. 9, 2012) (“Where, as here, a defendant does not obtain a plaintiff’s ‘personal information’ from a state motor vehicle agency, but instead, obtains that information directly from the plaintiff, any subsequent disclosure of that ‘personal information’ is not a DPPA violation.”); O’Brien v. Quad Six, Inc., 219 F. Supp. 2d 933, 934 (N.D. Ill. 2002) (“Reading the statute as a whole, it is clear that it is concerned with the source of the information—the state, as opposed to oneself—and not the medium by which it is conveyed—a driver’s license, passport, credit card, or the spoken word.”).

These interpretations run counter to a decision from the Northern District of Illinois. That court held that “[a] driver’s license number and the other information contained on a driver’s license is, without question, ‘part’ of a motor vehicle operator’s permit.” Pavone v. Law Offices of Anthony Mancini, Ltd., 205 F. Supp. 3d 961, 966 (N.D. Ill. 2016). Information from a driver’s license is, thus, information from a “motor vehicle record” and subject to DPPA protection. *Id.*

This court disagrees with *Mancini*. It treats the personal information on the license as the relevant “record.” The statute prohibits a person from “knowingly obtain[ing] or disclos[ing] personal information, from a motor vehicle

record,” 18 U.S.C. § 2722(a), with a “motor vehicle record” meaning “any record that pertains to a motor vehicle operator’s permit,” § 2725(1). To prevail on the claim, there should be, separately, “personal information,” a “record,” and a “motor vehicle operator’s permit.” *Mancini* treats the information on the driver’s license number as both “record” and “personal information.”

Strange and far-reaching results follow from the *Mancini* interpretation, treating the license as the “motor vehicle record,” or treating the “original source” as the BMV. Any non-excepted use of information pulled off a driver’s license provided by its holder would subject the user of that information to DPPA liability. The alleged violations of the Act in the appeals court cases described above—the *Fontanez* “new admirer” case and the *Best Buy* case—illustrate the absurdity and breadth of the resulting liability. Appriss points out other absurd results. For example, a person who uses information on her spouse’s driver’s license information to make an order or reservation would be liable to the spouse for a DPPA violation.² These results caution against conflating the various elements, or treating the DMV as the “original source” when the plaintiff discloses information. These interpretations balloon liability beyond the Act’s purpose of preventing disclosures by DMVs and misuse of information disclosed to third parties from DMVs.

The plaintiffs try to cabin the broad effects of these interpretations by arguing that the DPPA protects information on driver’s licenses only when that information is disclosed involuntarily. They argue that, because Indiana law

² That is, unless the spouse signed a written consent form. See 18 U.S.C. § 2721(b)(13).

requires disclosure of a driver's license to the police after an accident, the plaintiffs didn't disclose it voluntarily, so it remains under DPPA protection. Judge Moran arguably accepted this distinction when a night club patron's information was disclosed after she used her driver's license to gain access to the club. O'Brien v. Quad Six, Inc., 219 F. Supp. 2d 933, 935 (N.D. Ill. 2002) ("This statute seeks to control dissemination of information collected using the coercive power of the state. It does not regulate information freely given by consumers to private businesses"). The court declines to graft an involuntariness requirement onto the statute.

There's no strong basis for using voluntariness to determine DPPA coverage. No language in the statute alludes to this distinction. Even though this court disagrees with Judge Kennelly's conclusions in *Mancini*, both courts agree on this point. Pavone v. Law Offices of Anthony Mancini, Ltd., 205 F. Supp. 3d 961, 966 (N.D. Ill. 2016). Fact-intensive analysis of what disclosures are voluntary also provides little guidance to entities attempting to determine how to comply with the Act before disclosing data. If the voluntariness distinction were relevant, the evidence here wouldn't clearly answer whether the plaintiffs were required to disclose their licenses. Ms. Whitaker, for example, insisted that Officer Cunningham complete a police report. Could disclosure of her license be involuntary when she asked for the police report? It's unclear how a business like Appriss is to discern which data is voluntarily disclosed and so disclosable to others.

“Through passage of laws like the DPPA, Congress extended privacy rights beyond just those redressible at common law.” Whitaker v. Appriss, Inc., 3:13-cv-826, 2017 WL 193056, at *3 (N.D. Ind. Jan. 17, 2017). It did so narrowly and intentionally to protect information held by DMVs and disclosed by DMVs to other entities. *Id.* When the holder of a driver’s license hands over her personal information to an entity other than a DMV, even when that information is printed onto a driver’s license, the DPPA doesn’t protect it.

IV. CONCLUSION

Based on the foregoing, the court GRANTS Appriss’s motion for summary judgment [Doc. No. 175] and directs the Clerk to enter judgment accordingly.

SO ORDERED.

ENTERED: July 18, 2017

/s/ Robert L. Miller, Jr.
Judge
United States District Court