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-MGG
APPRISS, INC.,	)	
Defendant.	)	

OPINION AND ORDER

Defendant Appriss moves that the court dismiss the case for lack of subject-matter jurisdiction on the grounds that the named plaintiffs don't have standing to sue. Fed. R. Civ. P. 12(b)(1); U.S. Const. art. III, § 1. The court holds that the plaintiffs have standing and allows this case to proceed.

I. BACKGROUND

Plaintiffs Rachel Whitaker and Richard Dunkin allege the following. Each got into a car accident, after which the responding officer completed an Indiana Officer's Standard Crash Report. This report included the plaintiff's name, address, and driver's license number. The officer got this information from the plaintiff's driver's license and vehicle title information, both of which are maintained by the Indiana Bureau of Motor Vehicles. The accident report was then uploaded to www.buycrash.com.

Appriss runs this website. The company provides a uniform accident report for state agencies to use and software through which they can upload

completed reports. Parties involved in accidents can then buy copies of their accident reports on the website. Appriss also allows the public, including legal and medical professionals, to buy batches of reports or to subscribe, enabling them to use the personal information in these reports to solicit business.

Thirty days after their collisions, the plaintiffs began to receive solicitations in the mail. Both received letters from law firms referring to their accidents and advertising personal injury services. Ms. Whitaker also received an ad from a chiropractor. The plaintiffs believe that the businesses that solicited them acquired their reports from www.buycrash.com, learned about their accidents from those reports, and obtained their contact information from them.

The plaintiffs argue that Appriss violated the Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 *et seq.*, when it sold copies of accident reports containing personal information to third parties for solicitation purposes and without their consent. The plaintiffs didn't suffer monetary or physical harm from the sale of their personal information. They seek liquidated damages in the amount of $ 2,500 each, 18 U.S.C. § 2724(b)(1), and class certification.

The court bifurcated discovery, holding back the potential class action until the court determines whether the named plaintiffs prevail. While mid-discovery on the plaintiffs' claims, the court stayed proceedings pending the Supreme Court's decision in Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016), which would address Article III standing. After the Court decided Spokeo, the court extended the stay until it could determine if it had jurisdiction. Appriss moved to dismiss for lack of subject-matter jurisdiction. Fed. R. Civ. P. 12(b)(1).

II. STANDARD OF REVIEW

Plaintiffs' standing to sue implicates the court's subject-matter jurisdiction, so standing issues can be raised in a Rule 12(b)(1) motion. American Fed'n of Gov't Employees, Local 2119 v. Choen, 171 F.3d 460, 465 (7th Cir. 1999). The plaintiffs bear the burden of proving that they have standing. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-561 (1992). When considering a motion to dismiss for lack of standing, the court can look beyond the allegations of the complaint to other competent evidence. Bastuen v. AT&T Wireless Servs., Inc., 205 F.3d 983, 990 (7th Cir. 2000).

The plaintiffs must show that: (1) they suffered an injury in fact that's concrete and particularized and actual or imminent, not conjectural or hypothetical; (2) there's a causal connection between the injury and the conduct complained of; and (3) the injury can be redressed by a favorable decision. Lujan v. Defenders of Wildlife, 504 U.S. at 560-561 (1992). The second and third elements of standing are plainly met. Appriss contends that the plaintiffs don't allege "injury in fact" after Spokeo, and so they lack standing and this court lacks jurisdiction.

III. DISCUSSION

"[T]he injury-in-fact requirement requires a plaintiff to allege an injury that is both concrete *and* particularized." Spokeo v. Robins, 136 S. Ct. 1540, 1545 (2016). In Spokeo, the Supreme Court announced principles for determining "concreteness."

"A 'concrete' injury must be '*de facto*'; that is, it must actually exist." *Id.* at 1548. A "concrete" injury doesn't need to be tangible. In deciding whether an intangible injury is "concrete," first the court should consider "whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing basis for a lawsuit in English or American courts." *Id.* at 1549. Second, the court should look to Congress's judgment. "Congress may elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." *Id.* But a statutory violation alone doesn't necessarily exact concrete harm. *See id.* ("It is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."). "[B]are procedural violation[s], divorced from any concrete harm," also can't create an injury in fact. *Id.*

The plaintiffs aren't alleging a tangible injury. Both parties agree that the plaintiffs suffered no monetary, physical, or mental harm. Plaintiffs don't argue that the solicitations were particularly annoying or harassing. Plaintiffs just allege that Appriss violated their statutory rights under the DPPA when it disclosed their personal information, drawn from motor vehicle records, for unauthorized solicitation. 18 U.S.C. § 2722(a).

The first question then is whether this alleged "intangible harm has a close relationship to a harm that has traditionally been regarded as providing basis for a lawsuit in English or American courts." Spokeo v. Robins, 136 S. Ct. at 1549. Through the DPPA, Congress created rights "closely related" to the common law right to privacy. "Intrusion upon seclusion," one such privacy-based

tort, requires an intentional intrusion "upon the solitude or seclusion of another or his private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW INST. 1977). The common law right to privacy grew out of the right to be free from physical interference with body and property. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890), *cited by* RESTATEMENT (SECOND) OF TORTS § 652A cmt. a. Rights protected in statutes like the DPPA are natural outgrowths of the privacy-based torts of the common law. *See id.* at 193 ("Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.").

Today's personal data are held in myriad ways that are subtle and undetected, yet deeply penetrating. "We recognize, even if only intuitively, that our data has to be going somewhere. . . . Most of the time, we never think about this. We browse the Internet, and the data-collecting infrastructure of the digital world hums along quietly in the background." In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 266 (3d Cir. 2016). One of the driving forces behind passage of the DPPA was when an obsessive fan of television star Rebecca Schaeffer used her license plate number to obtain her address from the DMV and then gunned her down. *See* 140 CONG. REC. H2,518, 2,522, 2,526 (daily ed. April 20, 1994) (statements of Reps. Moran and Goss). That personal information is so readily accessible, and the kinds of nefarious purposes for which it can be used, might not be obvious or controllable to the average person. Congress recognized the potential harm such accessibility poses to our privacy and safety.

This case isn't framed as intrusion upon seclusion. Disclosure of personal information from an accident report obtained from a motor vehicle record might not be disclosure of a "private affair" "highly offensive to a reasonable person." *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. c ("[T]here is no liability for the examination of a public record concerning the plaintiff, or of documents that the plaintiff is required to keep and make available for public inspection.").

But Appriss confuses "close relationship" with sameness. *See* Potocnik v. Carlson, No. 13-cv-2093, 2016 WL 3919950, at *3 (D. Minn. July 15, 2016). Even if the plaintiffs don't think they were harmed monetarily or physically, they allege that Appriss, an entity properly entrusted with the personal information in their motor vehicle records, misused that information. If "close relationship" requires that the plaintiffs can plead a claim of intrusion upon seclusion, there would be little need for the DPPA.

The rights protected in the DPPA go beyond "intrusion upon seclusion" because they neither require proof that a disclosure is "highly offensive to a reasonable person" nor do they exclude public records. *See* Whitaker v. Appriss, Inc., No. 3:13-cv-826, Doc. No. 22, at *5 (N.D. Ind. Sept. 11, 2014). Through the DPPA, certain entities' classes of data use are effectively "highly offensive" *per se*. Personal information, while legally available to state departments of motor vehicles, is to be held in trust by them, disclosable only for certain prescribed purposes. Disclosure of that data breaches the trust and subjects persons to the risk that their data will be used against them. Further harm could take the form of something as mundanely annoying as junk mail or as serious as identity theft,

stalking, or battery. The DPPA purposes to combat all of these by preventing the kinds of disclosures that could lead to them. *See* Dahlstrom v. Sun-Times Media, LLC, 777 F.3d 937, 944 (7th Cir. 2015).

Through passage of laws like the DPPA, Congress extended privacy rights beyond just those redressible at common law. Disclosure of personally-identifying information is an inevitable facet of modern life, but certain forms of information are held in trust that it will be disclosed and used for narrow, authorized purposes alone.

"Congress may elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law." Spokeo v. Robins, 136 S. Ct. at 1548. That's exactly what happened here. The plaintiffs don't present an adequate claim for intrusion upon seclusion. Instead, the statute protects people from all knowing disclosure or obtainment of personal information from motor vehicle records, except in certain permissible instances. 18 U.S.C. § 2721-2722.

After Spokeo, not just any statutory violation confers standing. Certain types of violations simply can't work concrete harm. Spokeo v. Robins, 136 S. Ct. at 1550. Spokeo's example of this is an inaccurate zip code disclosed in the context of the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.* In interpreting Spokeo, our court of appeals similarly held that a store printing a customer's full credit card number on a receipt instead of just the last five digits, as required under the FCRA, didn't result in concrete injury. Meyers v. Nicolet Restaurant of De Pere, LLC, No. 16-2075, 2016 WL 7217581 (7th Cir. Dec. 13, 2016). In Meyers

no one saw the full credit card number on the receipt besides the plaintiff. *Id.* at *3. "[W]ithout a showing of injury apart from the statutory violation, the failure to truncate a credit card's expiration date is insufficient to confer Article III standing." *Id.* Harm to privacy needn't be great to confer standing, *see id.* at *3 n.5, but there must be some harm to privacy. If data is exposed and there's no one around to see it, a plaintiff can't sue about the exposure.[1]

Appriss argues that the plaintiffs allege nothing more serious than the incorrect zip code or the printing of a full credit card number on a receipt seen by the customer alone. But Appriss misses a primary purpose of the DPPA: data protection to prevent unwanted solicitation. Dahlstrom v. Sun-Times Media, LLC, 777 F.3d 937, 944 (7th Cir. 2015) ("Congress also enacted the DPPA to protect against the States' common practice of selling personal information to businesses engaged in direct marketing and solicitation.") (internal quotations omitted); 140 CONG. REC. H2,518, 2,522-23 (daily ed. April 20, 1994) (statement

[1] Another example mentioned by the parties is Gubala v. Time Warner Cable, Inc., No. 15-cv-1078, 2016 WL 3390415 (E.D. Wis. June 17, 2016), which interpreted Spokeo in the context of the Cable Communications Policy Act, 47 U.S.C. § 551. The CCPA requires cable operators to destroy personally identifiable information "[i]f the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information." 47 U.S.C. § 551(e). The plaintiff lacked standing because all he alleged was that the cable company held his information for longer than was allowed, a harmless act:

> He does not allege that the defendant has disclosed his information to a third party. Even if he had alleged such a disclosure, he does not allege that the disclosure caused him any harm. He does not allege that he has been contacted by marketers who obtained his information from the defendant, or that he has been the victim of fraud or identity theft.

Gubala, at *4. The plaintiffs here do allege disclosure to a third party for a prohibited purpose. This exposes them to risk of abuse. Not only that, but these plaintiffs allege that they've been contacted by marketers who impermissibly obtained that information.

of Rep. Moran) ("Marketers use DMV lists to do targeted mailings and other types of marketing. This amendment will allow them to continue to do so, as long as they agree not to market [to] drivers who object to their personal information being used for marketing purposes."). The analogous harmless DPPA violation wouldn't be the unauthorized spread of a person's name and address. It would be information that could never be used to identify or to cause physical or economic harm. An example would be the disclosure of a person's first name alone, without last name, address, or social security. This might violate the letter of the DPPA, but it presents no actual risk to privacy.

Further, in Meyers, "[t]he non-compliant receipt did not affect [the plaintiff's] behavior, nor did it create any appreciable risk that the concrete interest Congress identified (the integrity of personal identities) would be compromised." Meyers v. Nicolet Restaurant, 2016 WL 7217581, at *3 n.4 (7th Cir. Dec. 13, 2016). Ms. Whitaker and Mr. Duncan allege that, by selling their personal information to the general public for any purpose, Appriss created an appreciable risk that the concrete interest Congress identified (the integrity of personal identities) would be compromised. Entities allegedly bought the plaintiffs' information for a non-approved purpose, thus violating the privacy of the plaintiffs' information.

Spokeo doesn't overturn, but narrows, our court of appeals' earlier holding that impermissible disclosure of a plaintiff's personal information in violation of the DPPA confers standing. Graczyk v. W. Publ'g Co., 660 F.3d 275, 278 (7th Cir. 2011). Graczyk relied on Congress, through the DPPA, having defined a

particular injury in the form of the "'obtain[ment], disclos[ure], or [use],' 18 U.S.C. § 2724(a), of an individual's personal information." *Id.* Spokeo limits Graczyk to hold that Congress's judgment is "instructive and important" on whether an injury is concrete, but isn't necessarily sufficient. Graczyk's ultimate conclusion still survives but Spokeo just carves out completely harmless violations, such as the improperly disclosed first name described earlier.[2]

Appriss relies on Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013), *cited by* Spokeo v. Robins, 136 S. Ct. at 1544, for the proposition that "risk of real harm" is limited only to those harms that are "certainly impending." 133 S. Ct. at 1147. Appriss argues that because the plaintiffs allege, at most, to have received a few unauthorized solicitations, they don't allege a "certainly impending" threat in the form of monetary, physical, or emotional loss.

First, Clapper followed an "especially rigorous" standing requirement because the Clapper plaintiffs challenged the constitutionality of a federal law. Clapper v. Amnesty Int'l, 133 S. Ct. at 1147 ("[O]ur standing inquiry has been especially rigorous when reaching the merits of the dispute would force us to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional."). Ms. Whitaker and Mr. Duncan aren't challenging the constitutionality of the DPPA, but relying on it. Appriss does the opposite; it's not trying to use standing doctrine to shield congressionally-

[2] For the same reason, Spokeo similarly narrows, but doesn't overturn, our court of appeals' holding that "mere technical violation[s]" of the Video Privacy Protection Act, 18 U.S.C. § 2710, "(*i.e.*, impermissible disclosures of one's sensitive, personal information)" create an injury in fact. Sterk v. Redbox Automated Retail, LLC, 770 F.3d 618, 623 (7th Cir. 2014).

enacted law, but as a sword to limit the law's applicability. The "especially rigorous" approach of Clapper isn't warranted here.

Second, Appriss overlooks the kind of harm against which the DPPA protects. It protects against the "*obtain[ment], disclos[ure]*, or use[ ]" of personal information from motor vehicle records for a prohibited purpose. 18 U.S.C. § 2724(a) (emphasis added). In Congress's judgment, once a plaintiff's information is disclosed or obtained for a prohibited purpose, the damage is already done.

The Clapper plaintiffs didn't allege that their Fourth Amendment rights had already been invaded. Rather, their argument "rest[ed] on their highly speculative fear" that the government would target their communications for surveillance in reliance on the statute at issue and that the Foreign Intelligence Surveillance Court would approve the surveillance. Clapper v. Amnesty Int'l, 133 S. Ct. at 1148-1150. They didn't "face a threat of a certainly impending interception" of their communications pursuant to the challenged provision. *Id.* at 1152. The prohibited "interception" of Ms. Whitaker's and Mr. Duncan's information is alleged to have already occurred. Not only that, the plaintiffs' information is alleged to have been used for a prohibited purpose: the solicitations. In Clapper, the alleged Fourth Amendment violations weren't even "impending." In our case, the alleged violations have already occurred. Nothing more is needed.

The court of appeals adopted this position in *dicta*. In Lewert v. P.F. Chang's China Bistro, Inc., 819 F.3d 963 (7th Cir. 2016), the plaintiffs' credit card information was hacked at the defendant's restaurant. The hack in and of

itself wasn't enough to support standing. The court expressly distinguished the case from Sterk v. Redbox Automated Retail, LLC, 770 F.3d 618 (7th Cir. 2014), which "interpreted the Video Privacy Protection Act, 18 U.S.C. § 2710, which creates a legally protected interest in a consumer's personally identifiable information with respect to video rentals. *Sterk* does not recognize a legal interest in personally identifiable information beyond the video-rental context." Lewert v. P.F. Chang's, 819 F.3d at 968 (citations omitted). Just like the VPPA, the DPPA "creates a legally protected interest in a consumer's personally identifiable information." *Id.* In statutes like these, disclosing the personal information is the harm.[3]

A "bare procedural violation, divorced from any concrete harm," can't constitute injury in fact. Spokeo v. Robins, 136 S. Ct. at 1548. Because the substance of the statute itself is what's alleged to have been violated and it works a concrete harm, this isn't an issue.

The narrow standing rule that Appriss seeks seems to undo the statute on which the plaintiffs rely. As explained, one of the driving forces behind passage of the DPPA was an obsessive fan using now-DPPA-protected information to murder a celebrity. *See* 140 CONG. REC. H2,518, 2,522, 2,526 (daily ed. April 20,

[3] Even if the court characterizes the injury not as the disclosure itself, but as the risk that disclosure will result in more intense solicitation or crime, the plaintiffs still have standing. *See* Remijas v. Neiman Marcus Group, LLC, 794 F.3d 688, 693 (7th Cir. 2015) ("[T]he Neiman Marcus customers should not have to wait until hackers commit identity theft or credit-card fraud [after a data breach] in order to give the class standing, because there is an 'objectively reasonable likelihood' that such an injury will occur.") (quoting Clapper, 133 S. Ct. at 1147).

1994) (statements of Reps. Moran and Goss). The DPPA prohibits disclosure of personal data to prevent such injury before the fact. It would be odd for the court to require that a person whose information was unlawfully disclosed await such a grim result before suing. The Spokeo Court didn't mean to use a doctrine designed to prevent the judiciary from overstepping its bounds, *see* Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1146 (2013), to work such harm on a law Congress enacted to preserve individual privacy and safety.

Finally, *amici curiae* Hoosier State Press Association Foundation and Indiana Broadcasters Association argue that Indiana law guarantees that media outlets throughout Indiana have access to accident reports for their reporting. They say that if the plaintiffs have standing, this access will be compromised and could harm the press. There seems to be no conflict between Indiana law and the DPPA so long as DPPA-protected information is removed.[4] To the extent that there is conflict, Indiana law would be preempted. *See* Aux Sable Liquid Prods. v. Murphy, 526 F.3d 1028, 1032-1033 (7th Cir. 2008). *Amici* also argue that the

[4] There is no conflict between Indiana law and the DPPA. The state can still provide accident reports to the public as long as it removes DPPA-protected information.

Under Indiana law, a law enforcement officer must investigate each motor vehicle accident that results in injury, death, or property damage worth at least $1,000. Ind. Code § 9-26-2-1. The officer must prepare an accident report including the name and address of the owner and operator of the vehicle. § 9-26-2-2. The accident report isn't confidential and is available for inspection and copying under Indiana's Access to Public Records Act ("APRA"), Ind. Code § 5-14-3. § 9-26-2-3.

Under APRA, state agencies can't disclose public records "required to be kept confidential by federal law." § 5-14-3-4(a)(3). This would seem to exclude all DPPA-protected information. When "a public record contains disclosable and nondisclosable information," it must separate out the disclosable information. § 5-14-3-6. Accident reports could thus be made available to the press if and only if the state removed the DPPA-protected information from them. Last, a state agency may adopt an ordinance where electronic records are provided on condition that they can't be used to solicit. § 5-14-3-3(e). The BMV could require this of Appriss to facilitate DPPA compliance.

plaintiffs' position would open up media outlets to litigation whenever they obtain accident reports that happen to have DPPA-protected information. This is an issue of DPPA interpretation, not Article III standing, an issue it's too early to reach.

DPPA standing begins at least at the point of unlawful disclosure or obtainment of the plaintiffs' personal information. There's narrow exception for violations that are completely harmless because they provide information useless in identifying or seeking out the plaintiff. The alleged harm to Ms. Whitaker and Mr. Dunkin is thus "concrete." Under Graczyk v. West Publishing Co., 660 F.3d 275 (7th Cir. 2011), they meet the other elements of standing too. Assured of its subject-matter jurisdiction, the court allows this case to proceed.

IV. CONCLUSION

Based on the foregoing, the court DENIES Appriss's motion to dismiss for lack of subject-matter jurisdiction [Doc. No. 150] and ends the stay on proceedings.

SO ORDERED.

ENTERED: January 17, 2017

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