**UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT**
**(Case No. 18-55169)**

---

JAMES E. ANDREWS,
Individually and on behalf of all others similarly situated,

Plaintiff/Appellant

v.

SIRIUS XM RADIO, INC., DOES, 1-100 inclusive,

Defendants/Appellees

---

# APPELLANT JAMES E. ANDREWS' OPENING BRIEF

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF CALIFORNIA,
HONORABLE PERCY ANDERSON, PRESIDING
Case No. 5:17-cv-01724-PA-AFMx

**LAKESHORE LAW CENTER**
**JEFFREY WILENS (State Bar No. 120371)**
**18340 Yorba Linda Blvd., Suite 107-610**
**Yorba Linda, CA 92886**
**(714) 854-7205**
**(714) 854-7206 (fax)**

**Attorney for Appellant James E. Andrews**

# TOPICAL INDEX

# TABLE OF AUTHORITIES

## CASES

## STATUTES

Appellant and Plaintiff, JAMES E. ANDREWS, by and through his attorney, Jeffrey Wilens, hereby respectfully submits this Appellant's Opening Brief.

DATED: May 1, 2018

Respectfully submitted,

By _/s/_Jeffrey Wilens_____

JEFFREY WILENS
Attorney for Appellant

## STATEMENT OF JURISDICTION

The district court had jurisdiction over the original action pursuant to 28 USC § 1331, federal question. This court has jurisdiction pursuant to 28 USC § 1291 after entry of the final judgment following an order granting summary judgment. (Excerpts of Record[1] pp. 5-14.) The Notice of Appeal was filed on February 7, 2018. (ER pp. 1-2.) The appeal is timely pursuant to Federal Rules of Appellate Practice, Rule 4 (a) (2).

## STATEMENT OF ISSUES PRESENTED

I. DOES THE DRIVER PRIVACY PROTECTION ACT APPLY TO PERSONAL INFORMATION OBTAINED INDIRECTLY FROM A MOTOR VEHICLE RECORD AND IS A DRIVER LICENSE A MOTOR VEHICLE RECORD?

[1]Hereinafter ER.

II. SHOULD PLAINTIFF HAVE BEEN ALLOWED TO AMEND THE COMPLAINT TO PURSUE A CLAIM FOR VIOLATION OF THE COMPUTER FRAUD & ABUSE ACT WHERE DEFENDANT HACKED INTO A COMPUTER DATABASE AND STOLE PLAINTIFF'S VALUABLE PERSONAL INFORMATION?

## STATEMENT OF CASE

This is an appeal from entry of a final judgment of dismissal after granting of summary judgment for the defendant. The Complaint alleged a violation of the Driver Privacy Protection Act (DPPA), 18 USC § 2721 et. seq. Specifically, Respondent/Defendant Sirius XM (Sirius) was accused of knowingly obtaining personal information from a motor vehicle record without a permissible use in violation of 18 USC § 2722 (a).

Sirius moved for summary judgment. (ER, p. 241-257.) Plaintiff and Appellant James Andrews (Andrews) responded with both an opposition and a motion for leave to file a First Amended Complaint. (ER, 137-166; ER, 73-98.) The proposed First Amended Complaint would have added an additional claim for violation of the Computer Fraud & Abuse Act. (ER, pp. 84-98)

In its order granting summary judgment, the district court found that the undisputed facts showed there was no violation of the DPPA. The court also denied the motion to amend because it found adding a new claim under CFAA was "futile" in light of the court's finding that Andrews had not alleged that he and other persons suffered a "loss" of $5,000. (ER, pp. 5-14.) Andrews filed a timely appeal from the resulting judgment. (ER, pp. 1-2.)

## STATEMENT OF FACTS

The class action complaint alleged that Sirius acquired the name and address of persons who purchased cars equipped with SiriusXM radios from motor vehicle records and then sent marketing letters to them. (ER, pp. 283-284, ¶¶ 16-22.) This practice was alleged to be a violation of the Driver Privacy Protection Act (DPPA), 18 USC § 2721 et. seq.

Sirius XM operates a satellite digital radio service. Sirius XM offers subscriptions to owners and lessees of new and pre-owned, or used, vehicles. (ER, p. 259.) Andrews purchased a pre-owned 2012 Chevy Equinox from Auto Source, a vehicle

dealer in Banning, California on January 14, 2017, not January 15, 2017 as claimed by Sirius. (ER, p. 259.)

At the time of the purchase, and as required by the dealership, Andrews presented his California Department of Motor Vehicles driver license and signed a DMV Reg 262 form, "Vehicle/Vessel Transfer and Reassignment Form." The dealership got his name and PO Box address from the driver license. The dealership got his Nicolet street address from Andrews, who verbally provided that address and from the DMV form 262 which Andrews filled out. That is why DMV form 262 reflects both the physical and postal office addresses. The PO Box notated on the form 262 was written in by the dealership because both addresses should be on the DMV record. The dealership got his phone number from the form 262 as well. Andrews' name, one of his addresses, and his phone number were entered into the dealer management system (DMS) used by Auto Source. (ER, p. 259, 168.)

After the purchase, Sirius mailed 11 marketing solicitations to Andrews on January 16, 2017; February 20, 2017; March 13 and 23, 2017; April 17 and 18, 2017; May 3 and

24, 2017; June 11, 2017; July 18, 2017; and August 15, 2017. Sirius' telemarketing agents called Andrews at his phone number 11 times: on February 2 and 3, 2017; April 6, 2017; May 5, 15, and 18, 2017; and June 8, 9, 13, 19, and 20, 2017. (ER, pp. 259-260, 169.)

Although the complaint alleged that most likely Sirius got Andrews' personal information from motor vehicle records submitted to the DMV, it was discovered that Sirius had obtained his information from Auto Source's dealer management system (DMS). Sirius claimed that Sirius XM has agreements with automotive dealerships across the country pursuant to which dealerships provide the names, addresses, and phone numbers of consumers who purchase or lease pre-owned vehicles. (ER, p. 260.) Sirius claimed that Auto Source in Banning was one of the dealers with the contracts to provide customer information to Sirius XM (ER, p. 260). When Andrews purchased the Chevrolet Equinox, Sirius claims Auto Source sent an electronic record of that sale to Sirius XM that included Andrews' name, address and telephone number. (ER, pp. 260-261.)

While Sirius apparently obtained Andrews' information from Auto Source, the dealership provided it unwittingly and without its knowledge or consent. Auto Source officials denied they enrolled in any program or agreed to provide consumer information to Sirius XM. Auto Source officials denied they sent any electronic records or any customer information to Sirius XM. Instead, Sirius XM had some kind of back-door access to the DMS which Auto Source used to store the information obtained from Andrews. (ER, pp. 173-180, 182, 185.)

Once Auto Source discovered Sirius XM had a secret "back-door" access to its DMS, it terminated that access. Auto Source was upset about being tricked and the fact that customers' personal information was being taken and was not upset at the employee (as implied in the letter from Ms. Berger). (ER, pp. 184-185.)

Andrews never gave Auto Source any consent or permission to give his personal information (including name, address and phone number) to any third party except the DMV for purposes of registering and titling the vehicle. He never

gave his consent or permission for Sirius XM to access or obtain or use his personal information from the dealership's computer system or otherwise. (ER, p. 186.)

Based on the discovery of the secret back-door access to the dealership's computer, Andrews moved to file an amended complaint and asked the Court to deny summary judgment at least as to the additional claim. The proposed amended complaint, alleged in relevant part as follows:

> 18. Auto Source used a dealer management system (or dealer management software) (DMS) to store data pertaining to car inventory and sales. Some of this data was stored so it could be transmitted to the DMV in order to register vehicles that had been sold or leased. The DMS used by Auto Source was provided and/or hosted by AutoManager, Inc.
>
> 19. Auto Source required any consumer financing or leasing a vehicle to produce a current driver license or state identification card issued by the DMV. Auto Source also required consumers to complete a DMV Form 262 (transfer of title) form in connection with any purchase (including leases). Auto Source used personal information it obtained from the driver license and DMV form to enter data into the DMS.

20. Through methods described in greater detail in the next cause of action, shortly after the information was entered into the DMS, Defendant accessed Plaintiff's personal information (including his name, one of his two addresses, and his phone number as well as the VIN for the vehicle) stored on the DMS.

32. Auto Source did not authorize Defendant to access its DMS. As alleged above, Defendant was able to obtain "back door" access to the personal information stored in Auto Source's DMS. By "back door," Plaintiff means Auto Source did not transmit or send the information to Defendant. Instead, Defendant had some sort of arrangement with AutoManager that allowed it to access Auto Source's DMS without Auto Source knowing this was happening and without any involvement by Auto Source in the process.

34. Plaintiff is informed and believes, and thereupon alleges, that during the Class Period, Defendant obtained personal information about at least 200 persons who purchased or leased vehicles from Auto Source. These are the members of the Subclass.

35. The information Defendant obtained about Plaintiff and the Subclass members was extremely valuable to Defendant. The name, address and phone number of a person who just purchased or leased a vehicle equipped with a Sirius XM radio

(Defendant can tell from the VIN whether the vehicle has a Sirius XM radio) can and was used to aggressively market Defendant's subscription services. This information is what is called in the marketing industry a "hot lead." Plaintiff is informed and believes, and thereupon alleges, that the retail value of a "hot lead" of this nature and for the price point of Defendant's subscription plans is at least $100.

36. Plaintiff was the owner of his personal information stored on the DMS. While Plaintiff consented to Auto Source using that information to register the vehicle with the DMV, he did not consent to its use by any third parties for marketing purposes. Plaintiff appreciates the value of such personal information and would only have provided it to a third party if he was suitably compensated. Because Defendant stole the personal information without compensating Plaintiff, he lost the value of that information and the opportunity to sell it. Similarly, members of the Subclass were the owners of their personal information stored on the DMS and also lost the value of that information and opportunity to sell it when Defendant stole it.

37. Plaintiff is informed and believes, and thereupon alleges, that between November 21, 2016 and November 20, 2017, Defendant obtained the aforementioned valuable personal information belonging to at least 100

> persons, including Plaintiff, and that the aggregate value of that information was at least $5,000. (ER, pp. 89-94.)

The district court denied the motion to amend on the grounds that such amendment would be futile because the amended complaint failed to allege Andrews suffered a "loss" or "damage" cognizable under the CFAA. The district court granted the motion for summary judgment on the grounds that the DPPA did not apply to using personal information indirectly from motor vehicle records unless the information was obtained directly from the DMV. (ER, pp. 8-12.)

## STANDARD OF REVIEW

An order of dismissal after summary judgment is subjected to de novo review. The appellate court applies the same standard used by the district court: whether, viewing the evidence in the light most favorable to the nonmoving party, there are any genuine issues of material fact and whether the district court correctly applied the relevant substantive law. (San Jose Christian College v. City of Morgan Hill (9th Cir. 2004) 360 F.3d 1024, 1029-1030.) Evidentiary decisions made in the context of summary judgment motions are reviewed for

an abuse of discretion. (Block v. City of L.A. (9th Cir. 2001) 253 F.3d 410, 416.)

An order denying leave to amend the complaint is reviewed for an abuse of discretion, but such denial is strictly reviewed in light of the strong policy permitting amendment. (Ebner v. Fresh, Inc. (9th Cir. 2016) 838 F.3d 958, 963; Texaco, Inc. v. Ponsoldt (9th Cir. 1991) 939 F.2d 794, 798; Sisseton-Wahpeton Sioux Tribe of Lake Traverse Indian Reservation, North Dakota and South Dakota v. U.S. (9th Cir. 1996) 90 F.3d 351, 355.)

## SUMMARY OF ARGUMENT

The dismissal based on the order granting summary judgment must be reversed for two primary reasons. First, the district court erred by finding the Driver Privacy Protection Act does not actually protect the private information contained on a driver license, nor does it provide any protection for personal information from a motor vehicle record indirectly obtained by a company without the driver's consent. On a related basis, the district court failed to recognize there was a triable issue of fact whether a DMV form 262 that was also accessed by Sirius had

been transmitted to the DMV before the access occurred. For both reasons, summary judgment should not have been granted.

Second, the district court erred by denying a timely motion for leave to amend to add a viable claim for violation of the Computer Fraud & Abuse Act. Had the amendment been granted, summary judgment could not have been granted as that new claim was not the subject of the motion.

## ARGUMENT

### I. SUMMARY JUDGMENT SHOULD HAVE BEEN DENIED BECAUSE THE COURT CANNOT FIND AS A MATTER OF LAW THAT A PERSON IS LIABLE UNDER THE DPPA ONLY IF HE OBTAINS PERSONAL INFORMATION DIRECTLY FROM A STATE DEPARTMENT OF MOTOR VEHICLES RECORD, BECAUSE A DRIVER LICENSE IS A MOTOR VEHICLE RECORD AND BECAUSE THERE WAS A TRIABLE ISSUE OF FACT WHETHER DEFENDANT ACCESSED DMV FORM 262 AFTER IT WAS SUBMITTED TO THE DMV.

The Driver Privacy Protection Act (DPPA), 18 USC § 2721 et. seq. limits access and use of personal information contained in motor vehicle records. A major inspiration for the legislation was the murder of actress Rebecca Schaeffer by a stalker who had used DMV records to find her unlisted home address. The

legislative history reflects the concern for victims of crimes committed using DMV records. (Taylor v. Acxiom Corp. (5th Cir. 2010) 612 F.3d 325, 336.)

> The enactment of the DPPA responded to at least two concerns over the personal information contained in state motor vehicle records. The first was a growing threat from stalkers and criminals who could acquire personal information from state DMVs. The second concern related to the States' common practice of selling personal information to businesses engaged in direct marketing and solicitation." (Maracich v. Spears (2013) 570 U.S. 48, 57.)

Sirius argued, and the district court agreed, that the DPPA only limits disclosure of personal information when it is disclosed directly by the DMV and there is no permissible purpose for the disclosure. If the exact same information is disclosed on a driver license issued by a DMV the statutory protections do not apply. On a related note, Sirius argued, and the district court agreed, that a driver license is never a motor vehicle record and another form was accessed before it became a motor vehicle record (i.e. was transmitted to the DMV).

Andrews argues that the DPPA protects against misuse of

personal information found in motor vehicle records, including state issued driver licenses, regardless whether the information was obtained directly from a state DMV or provided by the driver to third parties. Andrews also argues a driver license is a motor vehicle record and the DMV form 262 might have been accessed by Sirius after it was transmitted to the DMV.

Since there is factual uncertainty regarding the final point, Andrews will focus on the primary questions—whether the DPPA only protects information found in records if the information is provided directly to a state DMV and whether a driver license is a motor vehicle record. On the final point, in light of the factual uncertainty, summary judgment should have been denied on that basis alone.

Regarding the primary questions, Andrews bases his argument on four points: 1) the express language of the DPPA permits liability to be based on disclosure of information from a motor vehicle record even if it was not obtained directly from the DMV; 2) the rule that a reviewing court must interpret an unambiguous statute literally unless doing so would produce absurd results or undermine the legislative intent; 3) the lack of

binding Ninth Circuit authority supporting the district court's interpretation; and 4) the fact that contrary authority from other circuits is distinguishable and/or unpersuasive.

### A. THE EXPRESS LANGUAGE OF THE DPPA PERMITS LIABILITY TO BE BASED ON DISCLOSURE OF INFORMATION FROM A MOTOR VEHICLE RECORD EVEN IF IT WAS NOT OBTAINED DIRECTLY FROM THE DMV.

The first part of the DPPA, 18 USC § 2721, regulates the conduct of state DMVs. It restricts such state agencies from knowingly disclosing personal information or highly restricted personal information to any person except for a "permissible use." (18 USC § 2721 (a).) Subdivision (b) lists numerous permissible uses, none of which are pertinent to this lawsuit. For that matter, § 2721 is not pertinent to this lawsuit except for the permissible use section which is incorporated by other provisions of the DPPA.

More to the point of this lawsuit is 18 USC § 2722, which provides:

> (a)Procurement for Unlawful Purpose. -
>
> It shall be unlawful for any person knowingly to obtain or disclose personal

> information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title.
>
> (b)False Representation. -
>
> It shall be unlawful for any person to make false representation to obtain any personal information from an individual's motor vehicle record.

This section is a general restriction on everyone and not just a state agency.

18 USC § 2723 (a) imposes a criminal fine on any person who violates any provision of the DPPA and a civil fine on a state DMV that has a policy of noncompliance.

The elements of the private cause of action are set forth in 18 USC § 2724:

> (a)Cause of Action. -
>
> A person who knowingly obtains, discloses or uses personal information, from a motor vehicle record, for a purpose not permitted under this chapter shall be liable to the individual to whom the information pertains, who may bring a civil action in a United States district court.
>
> (b)Remedies. -The court may award-
>
> (1) actual damages, but not less than liquidated damages in the amount of

> $2,500;
> (2) punitive damages upon proof of willful or reckless disregard of the law;
> (3) reasonable attorneys' fees and other litigation costs reasonably incurred; and
> (4) such other preliminary and equitable relief as the court determines to be appropriate.

Thus, to establish liability, a civil plaintiff must prove that the defendant 1) knowingly obtained or used personal information; 2) that the personal information came from a motor vehicle record and 3) that the defendant did not have a permissible purpose for obtaining or using the information. There is no requirement to prove actual damages as liquidated damages are available.

Finally, relevant definitions are found in 18 USC § 2725. "Personal information" means "information that identifies an individual, including an individual's ... name, address (but not the 5-digit zip code), telephone number..."(18 USC § 2725 (3).) A "motor vehicle record" means "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." (18 USC § 2725 (1).)

Liability in this case was actually fairly clear if the DPPA

requirements had been correctly interpreted. As to the first requirement, it was undisputed that Sirius obtained Andrews' personal information insofar as it obtained his "name." It also obtained an address for him, even though it had to update that address using other sources. It also obtained a telephone number. All that information qualifies as "personal information" under the DPPA.

It was also undisputed that Sirius used the personal information to send the marketing letters and make marketing phone calls. Presumably, Sirius knew it was using the personal information to send the mailings and it does not claim it got the personal information from any source other than the dealership. In any event, Sirius did not assert lack of knowledge as a basis for summary judgment so that requirement need not have been proven by Andrews.

Skipping to the third requirement, Sirius did not claim it had a permissible purpose or that marketing efforts are a permissible purpose.

Turning to the second requirement, it was also clear that Andrews' personal information came from a motor vehicle

record. 18 USC § 2725 (a) defines a motor vehicle record to including a "driver license" as well as any record pertaining to "registration."

Plaintiff argued there were two different motor vehicle records in play here. First, there was the DMV form 262, a change of ownership form that allow for registration of the vehicle to be put in the purchaser's name. Andrews presented evidence that his name, one of his two addresses, and a phone number were entered off the DMV form 262 into the dealership's computer system, where they were taken by Sirius.

Sirius denied the 262 form was a motor vehicle record, claiming that it had not yet been received by the DMV when Sirius acquired Andrews' personal information. (ER, p. 70.) The district court agreed. (ER, p. 9.) That ruling was also erroneous because there is a triable issue of fact as to **when** the DMV form was submitted to the DMV. Sirius' separate statement claims it acquired Andrews' information from the dealership's computer "on or about January 15, 2017." (ER, pp. 260-261.) The DMV form is dated January 14, 2017 but there is no evidence when it was received by the DMV. (ER, p. 190.)

The second motor vehicle record was Andrews' driver license. His name and his other addresses was copied off his driver license and entered into the dealership's DMS.

He presented both the driver license and signed DMV form 262 to the dealership as a mandatory part of the sales transaction.

In response, Sirius argued that it did not obtain Andrews' personal information directly from his driver license or the DMV form. Instead, it claims it got his personal information by accessing the dealer's computer system (apparently unbeknownst to the dealer). But Sirius did not dispute that the information in the computer system itself originally came from motor vehicle records.

So, confronted with the foregoing facts, Sirius presented an extremist argument. According to Sirius, it did not matter whether the personal information it obtained was copied off motor vehicle records; once the information was entered into the dealer's computer system, that information no longer constituted information from a motor vehicle record. Sirius argued that the DPPA only prohibits a person from obtaining

information directly from the DMV and it does not matter if he acquires personal information that came from a motor vehicle record presented by the driver to a different party, from whom Sirius got it.

But let us return to the express language of the statute. 18 USC § 2721 does in fact restrict conduct of state DMVs. But § 2721 is not the entirety of the DPPA. 18 USC § 2722 makes it unlawful to "obtain or disclose personal information, from a motor vehicle record, for any use not permitted under section 2721(b) of this title." This language does not say "to obtain or disclose personal information from a motor vehicle record *that was obtained directly from the department of motor vehicles*." Sirius convinced the district court to rewrite the statute to add the italicized words.

Moreover, the definition of a "motor vehicle record" includes any record that pertains to a "vehicle operator's permit," which is clearly a driver license. Nowhere in the definition does it say or even imply that the record must be obtained directly from the DMV. Additionally, the language is written broadly to include not only a driver license (for

example) but any record that pertains to it.

Furthermore, 18 USC § 2724 creates a private right of action against anyone who "knowingly obtains, discloses or uses personal information, from a motor vehicle record" without a permissible purpose. Again, the statutory language does not require that the personal information have come from the DMV itself or that the motor vehicle record (the driver license for example) be in the possession of the DMV at the time the defendant obtained the personal information. Had Congress intended to limit liability to those who obtain information directly from a state DMV, it could easily have inserted the words "directly from a state department of motor vehicles" into § 2724.

Indeed, what would be the point of the knowledge requirement if liability were limited to the situation where the defendant acquired the information directly from the DMV? In that case, the defendant would always know it received motor vehicle records. The knowledge requirement is put into place to protect a defendant who purchases or acquires personal information from a third party (not the DMV) and did not know

the information was based on motor vehicle records.

### B. THE COURT OF APPEALS SHOULD APPLY THE STATUTE LITERALLY.

As indicated above, Sirius convinced the district court to rewrite the statute or to interpret it in a way that greatly restricts its reach. This Court should overturn that restrictive interpretation.

If the language of a statute is unambiguous, the plain meaning controls. (United States v. Robinson (9th Cir. 1996) 94 F.3d 1325, 1328; United States v. Rrapi (9th Cir. 1999) 175 F.3d 742, 755.) "Statutory construction must begin with the language employed by Congress and the assumption that the ordinary meaning of that language accurately expresses the legislative purpose." (United States v. Havelock (9th Cir. 2012) 664 F.3d 1284, 1289.) "The plain language of a statute should be regarded as conclusive absent a 'clearly expressed legislative intention' to the contrary. (In re Hudson (9th Cir. 1988) 859 F.2d 1418, 1426.) It is not the job of a court to "rewrite" the law. "[T]he fact that Congress might have acted with greater clarity or foresight does not give courts a carte blanche to redraft statutes in an effort to achieve that which Congress is perceived

to have failed to do." (United States v. Havelock (9th Cir. 2012) 664 F.3d 1284, 1292.)

However, a court must "look beyond the express language of a statute where a literal interpretation 'would thwart the purpose of the over-all statutory scheme or lead to an absurd result.'" (Wilshire Westwood Assocs. v. Atlantic Richfield Corp. (9th Cir. 1989) 881 F.2d 801, 803-804, citing Brooks v. Donovan (9th Cir. 1983) 699 F.2d 1010, 1011.) Neither exception applies in the instant case.

As alluded to in the introduction, one major goal of the DPPA was to protect consumers from disclosure of sensitive information contained in motor vehicle records. The very title of the act is the "Driver's **Privacy Protection** Act." (emphasis added) Courts uniformly agree a purpose of the DPPA is to protect the privacy of drivers. (Maracich v. Spears, supra 570 U.S. 48 at p. 57; Taylor v. Acxiom Corp., supra, 612 F.3d at p. 336; Russell v. ChoicePoint Servs. (E.D.La. 2003) 300 F.Supp.2d 450, 45 (DPPA motivated by "mounting public safety concerns over stalkers' and other criminals' access to the personal information maintained in state DMV records");

Pichler v. Unite (3d Cir. 2008) 542 F.3d 380, 388 ("The DPPA provides redress for violation of a person's protected interest in the privacy of his or her motor vehicle records and the identifying information therein"); Collier v. Dickinson (11th Cir. 2007) 477 F.3d 1306, 1310 (enforcement provisions of the statute unambiguously focus on benefiting individuals and protecting their right of privacy). The DPPA sought to "strike a critical balance between an individual's fundamental right to privacy and safety and the legitimate governmental and business needs for this information." (Gordon v. Softech Int'l, Inc. (2d Cir. 2013) 726 F.3d 42, 50.)

A citizen suffers the same harm to his right of privacy and personal safety when his personal information contained in motor vehicle records is transmitted directly from the DMV to a marketing company as he would if the information were transmitted from motor vehicle records to one company and then retransmitted to the defendant. Information compromised is information compromised. If, at the end of the process the party in possession of the private information does not have a permissible purpose for possessing it, then the

overall statutory scheme should give the citizen legal recourse.

Nor would a literal reading of the statute produce absurd results. It is Sirius' reading that produces absurd results because a defendant would obtain immunity from liability for accessing personal information in motor vehicle records merely because it did not purchase the information directly from the DMV but instead acquired it from a business that legitimately got it from motor vehicle records.

Therefore, the Court must read 18 USC § 2724 literally. It creates a private right of action against anyone who "knowingly obtains, discloses or uses personal information, from a motor vehicle record" without a permissible purpose. The statutory language does not require that the personal information have come from the DMV itself or that the motor vehicle record (the driver license for example) be in the possession of the DMV at the time the defendant obtained the personal information.

### C. THERE IS NO BINDING PRECEDENT SUPPORTING DEFENDANT'S INTERPRETATION OF THE DPPA.

The district court made little effort to parse the statutory language. Instead, it cited superficially relevant cases, but

many of those opinions did not specifically address the question at hand.

For example, in Reno v. Condon (2000) 528 U.S. 141, the Supreme Court stated that the DPPA "restricts the States' ability to disclose a driver's personal information without the driver's consent" and "regulates the resale and redisclosure of drivers' personal information by private persons who have obtained that information from a state DMV." (Id. at p. 146.) This language was provided as background and not intended to define the **full parameters** of the DPPA. As pointed out by the court in Russell v. ChoicePoint Servs., supra, 300 F.Supp.2d at p. 461, "In Reno, the Supreme Court focused on the principles of federalism and the Tenth Amendment, not on the precise meaning and scope of the statute." Simply put, the Supreme Court did not rule that the DPPA only applies when a defendant has directly obtained motor vehicle records from a state DMV. That issue was not before the Court. The only issue before the Court was whether the DPPA as a whole was an unconstitutional interference with State functions.

There is not much authority in the Ninth Circuit.

Supporting Andrews' arguments, at least in part, is a preliminary ruling by the court in Wilcox v. Bastiste (E.D. Wash., June 9, 2017, No. 2:17-CV-122-RMP) 2017 WL 2525309, at *2.) That case involved the legality of selling accident reports that contained personal information about the drivers that was obtained from motor vehicle records. It is not fully clear from the decision whether it was driver licenses that were used to gather the information or DMV printouts of driver license information. Also, this ruling was one granting a preliminary injunction the discussion of the likelihood the plaintiffs would prevail was not a final ruling.

Nevertheless, the district court in Wilcox rejected at least one of the arguments made by Sirius in the instant case—that the DPPA only applies where a defendant has obtained information directly from a department of motor vehicles.

> In other words, WSP appears to argue that the DPPA protections do not apply to the information when that information is conveyed to a third party. . . .Although Defendants' proffered interpretation of the DPPA has received some support in case-law, . . .it appears to conflict with the plain language of the DPPA considered in context. Taken together, the DPPA's provisions seem to

> protect personal information if the original source of that information is a DMV database. (Id. at p. *2.)

In the instant case, the personal information obtained by Sirius came from a driver license, which ultimately was issued by the DMV, so the original source of the information would be the DMV.

As far as contrary Ninth Circuit authority, one case cited by Sirius was Lancaster v. City of Pleasanton (N.D.Cal. Sep. 13, 2013, No. C 12-05267 WHA) 2013 WL 5182949. In that case, the plaintiff alleged his ex-wife and others, including a law enforcement officer, conspired to defame him and cause his false arrest to gain leverage in a custody dispute. (Id. at p. *1.) The primary issue pertaining to the DPPA was whether "defendant's acquisition of plaintiff's motor vehicle records was for an improper purpose in violation of the DPPA." (Id. at p. *3.) The court concluded the information was obtained for a permissible purpose. (Id. at p. *4.) Further, the court concluded it was not likely the defendant acquired the information to instigate a police investigation because the information in the motor vehicle records were not of much use

for that purpose. Instead, as the plaintiff himself alleged, the defendant accessed other databases such as the California Law Enforcement Telecommunication System, National Crime Information Center, and CORPUS to gather evidence of prior criminal record, gang affiliation, etc. (Id. at p. *5.)

Sirius seized upon this language "the latter information obtained from databases other than the DMV is not protected information under the DPPA," (Id. at p. *4) but reads too much into it. The other databases did not contain motor vehicle records so of course DPPA does not apply. In the instant case, there is evidence the dealer's DMS did include motor vehicle records. Therefore, the foregoing language is not pertinent to the instant case.

The other case cited by Sirius was Chamber of Commerce of the United States v. City of Seattle (W.D.Wash. Apr. 4, 2017, No. C17-0370RSL) 274 F.Supp.3d 1140, 2017 U.S.Dist.LEXIS 51563. The issue there was a City ordinance requiring driver-for-hire companies (such as UBER) to disclose the names, contact information and driver license numbers for its drivers to the Teamsters Union so it could contact them to be

represented by the union. (2017 U.S.Dist.LEXIS 51563, at p. *2.) One of the challenges to the ordinance was that it violated the DPPA. A specific question arose whether the DPPA only applied to records obtained directly from the DMV or also applied if the information was obtained the from state-issued driver license. The court initially, in considering a request for a preliminary injunction, conceded that was a debatable point: "Whether information is universally protected from disclosure because it originated from the state department of motor vehicles, because it is in the possession of the state department of motor vehicles, or simply because it happens to be on a motor vehicle record (such as a license) is debatable." (Id. at p. *27.)

Some months later, the same court granted a motion to dismiss the DPPA claim. This is where the "baffling part" comes in. In dismissing the claim, the court reasoned:

> Plaintiffs do not allege that the for-hire drivers license or permit numbers that must be disclosed were issued by the state department of motor vehicles, are contained in its motor vehicle records, or are printed on their drivers' licenses. The implementing rules specifically require disclosure of licenses or

> numbers generated by King County and/or the City of Seattle, not the DMV. The allegations of the complaint do not, therefore, give rise to a plausible inference that the information that must be disclosed is "from a motor vehicle record" regulated by the DPPA. (Clark v. City of Seattle (W.D.Wash. Aug. 24, 2017, No. C17-0382RSL) 2017 WL 3641908, at *4, 2017 U.S.Dist.LEXIS 136322, at *14.)

It is difficult to make sense out of the court's comment that "Plaintiffs do not allege" that the license numbers "were issued by the state department of motor vehicles, are contained in its motor vehicle records, or are printed on their drivers' licenses." If the license numbers were not issued by the DMV and printed on the driver licenses, then where did they come from? Andrews doubts that UBER can issue a driver license number. Presumably, the explanation is that the plaintiff in that case backed off its prior allegations that the information came from a driver license. Maybe the drivers just verbally gave the information to UBER, which then recorded it in its own database.

In any event, these two decisions are not of much help to the Court due to confusion over the facts as stated and because

in the instant case, Andrews has presented evidence he did give his physical driver license to the dealership and that he dealership copied that information into its DMS.

### D. THERE IS A SPLIT OF AUTHORITY OUTSIDE THE NINTH CIRCUIT BUT THE RULINGS SUPPORTING DEFENDANT'S POSITION ARE NOT PERSUASIVE.

There is some authority supporting Andrews' argument. The leading case in Andrews' favor is Pavone v. Law Offices of Anthony Mancini, Ltd. (N.D.Ill. 2016) 205 F. Supp. 3d 961. In that case, the plaintiff was involved in a car accident and was required to produce his driver license to the investigating officer at the scene. The officer recorded his personal information from the driver license onto the crash report. (Id. at pp. 962-963.) Subsequently, a third party was permitted by the police to publish accident reports on its site. A trolling personal injury lawyer purchased the report and mailed a solicitation letter to the plaintiff, who sued the lawyer under the DPPA.

The court upheld the DPPA claim. First, the court agreed that the information recorded (including the driver's name) was

personal information under the DPPA. (Id. at pp. 963-964.)

Second, it agreed that § 2724 must be read literally. While § 2721 limits liability to state DMVs or persons who acquire information directly from state DMVs, § 2722 and § 2724 are not so limited. The court noted that given the wording of the statute, "even if a document is created by the police, the DPPA protects any information in the report that the police obtained from the motor vehicle record." (Id. at p. 964.)

Along the same lines, the court made this excellent point:

> [T]he Court sees no appropriate basis in the language of the statute to read the term "from a motor vehicle record" to limit liability to situations involving disclosure or use of personal information that the defendant himself got directly from a state department of motor vehicles. Among other things, were this the case, there would be no need for section 2724(a) to limit liability to persons who "knowingly" obtain or use personal information from a motor vehicle record—because a person who gets the information directly from a state agency quite obviously knows that is where he is getting the information. (Id. at p. 965.)

Third, the court agreed that "information obtained from a driver's license is information obtained from a motor vehicle

record." (Id. at p. 966.)

This case matches up with the facts of the instant case. Here, Andrews produced his driver license because it was required to buy the car. Information off his driver license (as well as off another DMV form) was put into Auto Source's DMS. There is a dispute concerning whether or not Sirius XM acquired the information off the DMS with the dealer's consent or stole it. In any event, just like the personal injury lawyer in Pavone, Sirius XM then aggressively trolled Andrews to sign up for Sirius' subscription radio service.

Additional supporting authority is found in Garey v. Farrin (M.D.N.C., Sept. 29, 2017, No. 1:16CV542) 2017 WL 4357445 and its companion case Hatch v. Demayo (M.D.N.C., Sept. 29, 2017, No. 1:16CV925) 2017 WL 4357447. The lawsuits were brought by persons involved in motor vehicle accidents. As part of the police investigations of the accidents, the officers reviewed the driver licenses and recorded the information onto the accident reports. The defendants, local law firms, purchased the accident reports and then mailed advertisements for their legal services to the accident victims

identified in the reports. (Garey, 2017 WL 4357445, *1-2; Hatch, 2017 WL 4357447, *1-2.)

The law firms moved to dismiss raising arguments similar those raised by Sirius. In rejecting those arguments, the district court made the following points:

The argument that the DPPA only applies to records directly provided to the defendant by a state DMV was rejected because 18 USC § 2724 expands liability to any person who obtains motor vehicle records by any means. (Garey, supra, 2017 WL 4357445, *8; Hatch, supra, 2017 WL 4357447, *7.)

The argument that an accident report is not a motor vehicle record ignores the fact that the information from the motor vehicle record (driver license) is printed in the accident report. (Garey, 2017 WL 4357445, *8; Hatch, 2017 WL 4357447, *7.) Similarly, the record obtained by Sirius from the dealership's computer is not a motor vehicle record, but it did contain information from a motor vehicle record.

Finally, in Moncier v. Harris (Tenn. Ct. App., Apr. 5, 2018, No. E201600209COAR3CV) 2018 WL 1640072, at *8, the Tennessee appellate court interpreted a state statute that

used the same definition of a motor vehicle record found in the DPPA and found that a driver license was a motor vehicle record under that same definition.

The district court rejected the ruling in Pavone and presumably would have rejected the rulings in the North Carolina district court cases, on two grounds.

First, the district court drew a distinction between a record that pertains to a motor vehicle operating permit and a motor vehicle operating permit (driver license) itself. As noted earlier, a "motor vehicle record" is defined as "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." (18 USC § 2725 (1).) From this the court reasoned:

> Similarly, a driver license, although it contains "personal information" contained in the records of the DMV, is not itself a "record" "contained in the records" of the DMV. Nor does it make sense to include a driver license as a "motor vehicle record" when a "motor vehicle record" is defined as "any record that pertains to a motor vehicle operator's permit." Interpreting the statute as Plaintiff suggests and construing a "motor vehicle record" to

> include a driver license would render the definition's use of both "record" and "pertains to" as surplusage because the driver license would be "pertaining" to itself and ignore the requirement that is also be a "record." (ER, p. 9.)

Sirius argued the "pertains to" language would be superfluous if Congress had meant for a driver license itself to qualify as a motor vehicle record. The statutory definition could have been written clearer. For example, it could have been written: "any record *including or pertaining to* a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles." However, as written it is not ambiguous nor are the words "record" and "pertains to" superfluous even if they are partially redundant.

If you delete the "pertains to" language then nothing is left to be a motor vehicle record. Adding the "pertains to" language does not rule out a driver license from being a motor vehicle record, but instead uses that as an example while expanding the universe of records subject to the DPPA. A driver license is a motor vehicle record, but the definition was intended to broadly sweep in any other document "pertaining

to" a driver license as well. For example, a printout of a driver license would be a record pertaining to the driver license. Partially redundant or not, there was no legal justification to simply eliminate a driver license as a motor vehicle record. If that was intent, the language would have expressly excluded a driver license.

Yet, under the district court's reasoning, if a stalker obtained a person's home address from a DMV printout containing the same information as found on the driver license, there would be liability under the DPPA. But if he simply was able to order a duplicate driver license from the DMV to get the same information there would be no liability. What rational basis would Congress have had for allowing stalkers to obtain a printout of a driver license but not a DMV document containing information from a driver license? How would such a distinction address the fundamental purpose behind the DPPA?

Sirius and the district court cited the similar distinction that was made in Whitaker v. Appriss, Inc. (N.D. Ind. 2017) 266 F.Supp.3d 1103, dismissed (7th Cir., Nov. 8, 2017, No. 17-2679) 2017 WL 7689606. That court held that a company could sell

accident reports even though the reports contained personal information scanned from the driver licenses of the drivers involved in the accident. Unlike the Pavone and Garey/Hatch courts, the Appriss court made an arbitrary distinction between information obtained from a driver license turned over by driver and information obtained from a record of the driver license held in the database of the state DMV. (Id. at p. 1107.) This distinction makes no sense. A driver license is the property of the state DMV. If it were otherwise, the State would not have the right to issue or confiscate it. What possible real difference does it make whether a picture of the driver license is downloaded from the DMV website as oppose to scanned in manually by the police officer who demanded the license be produced by the driver?

Second, the district court reasoned that to accept Andrews' reasoning would lead to absurd results or as the court in Whitaker v. Appriss, Inc., supra, put it, "strange and far-reaching results." (Id. at p. 1109.) These concerns are gravely overblown and do not justify gutting the DPPA's protections.

The example of an "absurd result" cited by the district

court was that a Good Samaritan who finds a lost wallet and uses the name and address found on the driver license in the wallet to return the wallet to its owner would face criminal and civil liability. (ER, p. 9.)

The Good Samaritan scenario is a straw man argument because Good Samaritans are exempt from liability for numerous acts that would otherwise be treated as criminal or civil violations. It is illegal to intentionally break another person's window, but there is a common law exception for doing so to save his life. It is illegal to kiss another person without consent or squeeze her (battery) but giving mouth to mouth resuscitation or performing the Heimlich maneuver on an unconscious choking victim would be permitted. Opening a lost wallet and reading the driver license to identify the owner cannot possibly expose the Good Samaritan to liability under the DPPA for the same reasons Good Samaritan conduct would not in the other circumstances.

Moreover, the court's scenario proves too much. The court posits it is necessary to exclude driver licenses from constituting motor vehicle records to avoid affixing liability to

"innocent conduct." But what if the Good Samaritan found a lost wallet that contained not a driver license, but an official motor vehicle record itself, fresh from the DMV printer, as the wallet belonged to a DMV official who happened to print his driver license history that day. Presumably, everyone would agree that the Good Samaritan knowingly used a motor vehicle record in these circumstances and the problem cannot be "defined away" by excluding driver licenses.

Still, most would agree there was no liability but not through the trick of defining away the problem. Instead there would be no liability because there is a common law necessity defense at play that underlays the Good Samaritan doctrine. The solution to obscure scenarios such as the hypothetical presented by the district court is to apply principle such as the Good Samaritan doctrine rather than twist the law.

Other courts posit different examples of the "absurd results" that would supposedly occur if a driver license were viewed as a motor vehicle record. The court in Whitaker v. Appriss, Inc., supra, cited this scenario from Fontanez v. Skepple (2d Cir. 2014) 563 Fed.Appx. 847, 848: a woman

visiting her boyfriend in jail presented her driver license as proof of identity to the guard. The corrections officer noted her address and later sends her a "teddy bear" from her "new admirer." Supposedly imposing liability on this creep would be an absurd result, according to the Whitaker court but that is certainly debatable.

In any event, there is a big distinction between the guard using the information that was voluntarily submitted to him and a third party who was never given any kind of consent to use the information. In the instant case, Andrews did not sue the dealership to whom he gave his driver license to purchase a car. He sued Sirius which hacked into the dealership's computer to obtain the information from the driver license.

Another supposed example of an absurd result cited by the Appriss court was where a person "uses information on her spouse's driver's license information to make an order or reservation" and therefore "would be liable to the spouse for a DPPA violation." (Whitaker v. Appriss, Inc., supra, 266 F.Supp.3d at p. 1109.) But presumably the spouse acted with consent in using information from the driver license to make a

purchase. There is no liability for using a driver license to make a purchase as the spouse would be acting as an agent of the licensee.

On the other hand, let's imagine the spouses were estranged and the husband stole his wife's driver license to make a purchase for himself without her consent. In what way would it be absurd to prosecute the husband for a violation of the DPPA?

A final example of an "absurd result" according to Sirius pertains to the fact the court docket in this case now contains a partially redacted picture of Andrews' driver license. According to Sirius, this means that "anyone obtaining that information for a purpose not qualifying for a statutory exception would—under Plaintiff's theory—violate the statute." (ER, p. 71.) No, such persons obviously would not be violating the statute as Plaintiff would have waived any privacy expectations having consented to publication of his driver license. On the other hand, if someone stole Plaintiff's wallet so they could have look at his driver license to discover his address, that would be a violation of the DPPA.

Sirius primarily relied on unpersuasive rulings from other jurisdictions. The leading case cited by Sirius is Siegler v. Best Buy Co. of Minn. (11th Cir. 2013) 519 F.App'x 604. In that case the plaintiff purchased a computer mouse from Best Buy. The following day, he returned the item and a store cashier requested Siegler's driver's license to complete the return. Siegler voluntarily presented his license to the cashier, who then scanned the magnetic strip on his license "without warning." Siegler demanded that the information from the magnetic strip be deleted, but Best Buy said it was unable to do so

In cursory fashion, the 11th Circuit held the DPPA did not apply:

> A plain reading of the DPPA makes clear that the Act was intended to prohibit only the disclosure or redisclosure of information originating from state department of motor vehicles ("DMV") records. The thrust of the Act is contained in § 2721, which prohibits a state DMV, and any officer, employee, or contractor thereof, from knowingly disclosing "personal information" or "highly restricted personal information" contained in motor vehicle records, except for a limited number of "permissible uses." §§ 2721 (a) and (b).

> In turn, § 2721 (c), entitled "resale or redisclosure," restricts the redisclosure of information obtained from a state DMV to limited circumstances by recipients authorized to receive disclosures under § 2721(b). On its face, the Act is concerned only with information disclosed, in the first instance, by state DMVs. (Id. at p. 605.)

To the contrary, a plain reading of § 2724 does not require that the personal information from a motor vehicle record had been transmitted directly from the DMV to Best Buy. The 11th Circuit completely ignored § 2724 and did not support its assumption that the DPPA is only concerned with information disclosed by state DMVs. That assumption requires rewriting § 2724 to add the words "from the DMV" to the phrase "personal information, from a motor vehicle record."

In any event, there is an important distinction between the facts in Siegler and those in the instant case. In Siegler, the plaintiff sued Best Buy even though he provided his driver license to obtain the refund. While Best Buy scanned in the data, there is no evidence anyone other than Best Buy saw or used it. By contrast, Andrews is not suing Auto Source to whom he gave his driver license in order to buy the car. He is suing an

unrelated third party who accessed information from his driver license without consent and used it for an impermissible purpose.

Another case cited by Sirius is also similar to the instant one but with the same important distinction. In O'Brien v. Quad Six, Inc. (N.D.Ill. 2002) 219 F.Supp.2d 933, 933, the plaintiff gave his driver license to a nightclub attendant to gain entrance. The nightclub videotaped his license and entered the personal information into its computer system and then shared that information with another nightclub it owned. The court held the DPPA did not apply because "Defendants did not obtain plaintiff's information (his name and address) from a state motor vehicle agency. Plaintiff himself presented his driver's license to nightclub personnel as identification." (Id. at p. 934.)

The court rejected the argument that § 2724 did not require the personal information come "from a state agency." The court believed the statute was only to regulate "information collected from citizens by the state, not transactions between private businesses and their customers." (Id. at p. 934.)

However, contrary to the reasoning presented in the O'Brien case, Congress was not just concerned with the conduct of the state; it was concerned with the privacy rights of the citizens and specifically addresses their privacy rights as pertaining to their driver license. Congress was also concerned about stalking. One business indiscriminately sharing information from motor vehicle records with another business increases the risk of the information falling into the wrong hands.

The O'Brien court rather simplistically stated that "Consumers who do not want private businesses to use their personal information can simply decline to disclose it and can refuse to patronize businesses that demand such information as a condition of service." (Id. at p. 934.) In the real world, consumers who want to open a bank account, purchase a car or do any number of other things have no choice but to produce a driver license or other state issued identification card. Moreover, if one business with a legitimate need to copy information from a driver license secretly transfers the information to a third party, how is the consumer supposed to know that is even happening?

Sirius also relied on the Second Circuit decision in Fontanez v. Skepple, supra, mentioned previously, another cursory decision which also concluded, without any consideration of the express language of § 2724, that the DPPA does not apply unless the personal information is obtained directly from a state DMV. The Fontanez court cited two earlier Second Circuit decisions. One was Figueroa v. Taylor (S.D.N.Y., Oct. 23, 2006, No. 06 CIV. 3676 PACKNF) 2006 WL 3022966, at *4, which asserted that to establish a claim under the DPPA the plaintiff must show that "the defendants caused a DMV search to be made." Figueroa's holding can be traced back to Cowan v. Ernest Codelia, P.C. (S.D.N.Y. 2001) 149 F.Supp.2d 67, 78, which gave no explanation for this faulty assertion. There is nothing in § 2724 that requires a plaintiff to prove a "DMV search" was conducted. The other case cited by the Fontanez court was Ocasio v. Riverbay Corp. (S.D.N.Y. June 19, 2007) 2007 WL 1771770, at *1, which falsely asserted that the Supreme Court ruled in Reno v. Condon, supra, the DPPA only applies where the defendant "obtained the information from a state motor vehicle agency." That is a misreading of Reno,

supra as discussed above.

Sirius also cited Hurst v. State Farm Mut. Auto. Ins. Co. (D.Del. Feb. 9, 2012, No. 10-1001-GMS) 2012 WL 426018, at *10 (requiring proof defendant caused a DMV search to be made). But the sheer quantity of unpersuasive rulings, especially against pro se plaintiffs, misconstruing the express language of § 2724 should not carry the day for Sirius.

This is an area of law where Congress wrote a clear statute, but many lower courts have arbitrarily castrated it. In as much as there is no binding United States Supreme Court or Ninth Circuit authority, this Court is free to exercise its own independent judgment, which should be tempered by the fundamental rule that a judge's function is to apply a statute as written and not to be a legislator.

In performing that function, this Court should issue a limited ruling holding that where a plaintiff can establish that a third party accessed a report (whether it be an accident report or dealership record of sales) containing information from a driver licensed issued by a state DMV, and where the third party did not have consent from the plaintiff nor was acting on

his behalf, and where the third party used the information for marketing purposes, the plaintiff can state a claim for violation of the DPPA. Under such a limited ruling, the judgment must be reversed as there were triable issues of fact.

## II. SUMMARY JUDGMENT SHOULD HAVE BEEN DENIED BECAUSE THERE ARE ADDITIONAL THEORIES OF LIABILITY WHICH ANDREWS SHOULD HAVE BEEN GIVEN TIME TO PLEAD AND CONDUCT DISCOVERY ON.

As noted above, based on information learned after the motion for summary judgment was filed, Andrews moved to amend the complaint to add a claim under the Computer Fraud & Abuse Act. As the deadline to amend the complaint had not yet been reached, no issue was raised about the timeliness of the amendment. Instead, the sole ground for denying the motion to amend was "futility."

The CFAA creates criminal liability for any person who, among other conduct, "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 USC § 1030(a)(2)(C). The CFAA also establishes the right to bring a civil claim by "[a]ny person who suffers damage or loss

by reason of a violation of this section . . . against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 USC § 1030(g). "A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)." Id. The factors described in subclauses (I) through (V) of subsection (c)(4)(A)(i) involve:

> (I) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value;
> (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
> (III) physical injury to any person;
> (IV) a threat to public health or safety; [or]
> (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security. (18 USC § 1030(c)(4)(A)(i).)

The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 USC § 1030(e)(8). Under the CFAA, "'loss' means any reasonable cost to any victim, including the cost of

responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 USC § 1030(e)(11).

The only deficiency in pleading relied upon by the court in denying the amendment was the failure to plead Andrews suffered any cognizable "loss." If "loss" was shown, there was no need to provide "damage."

Andrews presented uncontested evidence of loss, which was the marketing value of his personal information. The $5,000 loss is in the aggregate for multiple persons. Andrews has pled more than 100 victims so individual loss need only be $50.

Andrews pled that Sirius stole valuable personal information about him, namely that he had just purchased a particular vehicle equipped with a Sirius XM radio system, as well his contact information. There is no conceivable way Sirius could have known that if it had not hacked into the dealership's computer system. Andrews characterizes this recent purchase

information as a "hot lead" and alleges its value in the advertising/marketing world was at least $100 per consumer. (ER, p. 93.) Obviously, it was valuable to Sirius, which used it to spam Andrews with emails and phone calls offering Sirius' services.

Andrews was not willing to give this information away, but he would have for compensation. Because Sirius stole the personal information without compensating Andrews, he lost the value of that information and the opportunity to sell it. Similarly, other consumers who were the owners of their personal information stored on the DMS also lost the value of that information and opportunity to sell it when Sirius stole it. (ER, pp. 93-94.)

The district court adopted a hyper-technical interpretation of "loss" that was contrary to the Ninth Circuit decision in Creative Computing v. Getloaded.com, LLC (9th Cir. 2004) 386 F.3d 930, which is controlling. The district court did not even address that decision.

In that case, a company was able to log into a competitor's website posing as a legitimate customer and obtain valuable

information about its marketing practices. The Court upheld the CFAA claim against a similar argument that there was no "loss."

> Getloaded objects to paying damages for loss of business and business goodwill. The objection is without force because those are economic damages. The statutory restriction, "limited to economic damages," precludes damages for death, personal injury, mental distress, and the like. When an individual or firm's money or property are impaired in value, or money or property is lost, or money must be spent to restore or maintain some aspect of a business affected by a violation, those are "economic damages." The same result is compelled under both the old and new versions of the statute. (Id. at p. 935.)

See also, Ervin & Smith Advertising and Public Relations, Inc. v. Ervin (D. Neb., Feb. 3, 2009, No. 8:08CV459) 2009 WL 249998, at *9 (CFAA still applies where there is a loss of revenue even without physical damage to a computer or interruption of service); CoStar Realty Information, Inc. v. Field (D. Md. 2009) 612 F.Supp.2d 660, 675 (finding loss of revenue arising from unauthorized access to computer system qualified as damages under CFAA).)

Sirius attempted to escape the force of this holding by arguing "any claim of personal injury due to any claimed diminution in value of his personal information—unlike a loss of business—would not count as 'economic damages'." (ER, p. 42, n. 2.) However, Andrews was not claiming "personal injury" or the like. His claim was based on the misappropriation of the market value of the information about his car purchase and was not a personal injury claim. It is a claim based on loss of the commercial value of his information. The fact Andrews is a natural person and the plaintiff in the Creative Computing case was a corporation cannot make any difference in application of the CFAA, which allows "any person" to bring a claim. Moreover, the Creative Computing decision specifically recognized that both an "individual" and "firm" can suffer economic damages in this manner.

It is true that some courts have rejected a plaintiff's generalized claim that loss of the marketing value of personal information constitutes economic loss under CFAA. (See e.g., In re iPhone Application Litig. (N.D.Cal. 2012) 844 F.Supp.2d 1040, 1068.) However, in those cases, the value was purely

speculative because it was not linked to actual marketing activity. (Del Vecchio v. Amazon.com Inc. (W.D.Wash. Nov. 30, 2011, No. C11-366-RSL) 2012 WL 1997697, at *4.) In the instant case, there is a direct link between the acquisition of Andrews' time-sensitive personal information and the marketing activity. Andrews bought the car on January 14, 2017 and Sirius sent the first targeted advertisement to him on January 16, 2017. Sirius mailed a total of 11 targeted advertisements and made 11 telemarketing calls through August 2017. (FAC, ¶ 21.) This suggests the personal information had a verifiable marketing value, which was diminishing over time, and makes the loss concrete and not speculative.

Since Andrews could plausibly allege a viable alternative theory of liability and since he was still permitted by the case management order to amend the complaint, the motion to amend should have been granted. No matter how this Court rules on the DPPA claim, the judgment must be reversed, and Andrews must be given a reasonable opportunity to conduct discovery and pursue the alternative theory.

## CONCLUSION

For the foregoing reasons, this Court should reverse the district court's order granting summary judgment and denying the motion to amend.

DATED: May 1, 2018

Respectfully submitted,

By _/s/_Jeffrey Wilens_____

JEFFREY WILENS
Attorney for Appellant

## STATEMENT OF RELATED CASES

None.

## CERTIFICATE OF COMPLIANCE

I, Jeffrey Wilens, do hereby certify the following:

Pursuant to the Federal Rules of Appellate Procedure Rule 32 (a) (7) (C) and Ninth Circuit Rule 32-1, the attached opening brief was prepared with Microsoft Word 2007, is proportionately spaced, has a typeface of 14 points or more and contains approximately 10,796 words (not exceeding 14,000) excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed this 1st day of May 2018 at Yorba Linda, California.

_/s/_Jeffrey Wilens_____

Jeffrey Wilens

## CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on May 1, 2018.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

____/s/_Jeffrey Wilens_____

Jeffrey Wilens