FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

JAMES E. ANDREWS, on behalf of himself and all persons similarly situated, *Plaintiff-Appellant*, v. SIRIUS XM RADIO INC.; DOES, 1 through 100, inclusive, *Defendants-Appellees.*	No. 18-55169 D.C. No. 5:17-cv-01724-PA-AFM OPINION

Appeal from the United States District Court
for the Central District of California
Percy Anderson, District Judge, Presiding

Argued and Submitted July 10, 2019
Pasadena, California

Filed August 8, 2019

Before: MILAN D. SMITH, JR. and MICHELLE T. FRIEDLAND, Circuit Judges, and STANLEY A. BASTIAN,* District Judge.

Opinion by Judge Milan D. Smith, Jr.

---

* The Honorable Stanley A. Bastian, United States District Judge for the Eastern District of Washington, sitting by designation.

SUMMARY[**]

Driver's Privacy Protection Act

The panel affirmed the district court's grant of summary judgment in favor of the defendant in an action under the Driver's Privacy Protection Act, which prohibits the use and disclosure of personal information derived from Department of Motor Vehicles records.

After the dealership from which plaintiff bought a used car provided his personal information to defendant Sirius XM Radio, Inc., plaintiff received unsolicited advertisements asking him to renew his radio subscription. The panel held that the DPPA does not apply where the source of personal information is a driver's license in the possession of its owner, rather than a state Department of Motor Vehicles. The panel therefore affirmed the district court's grant of summary judgment.

The panel further held that the district court did not abuse its discretion in denying plaintiff leave to amend his complaint to add a claim under the Computer Fraud and Abuse Act. The panel held that plaintiff could not have brought a viable CFAA claim because he could not plausibly allege a qualifying loss.

[**] This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

COUNSEL

Jeffrey Wilens (argued), Lakeshore Law Center, Yorba Linda, California, for Plaintiff-Appellant.

Shay Dvoretzky (argued) and Jeffrey R. Johnson, Jones Day, Washington, D.C.; Thomas Demitrack, Jones Day, Cleveland, Ohio; Lee A. Armstrong, Jones Day, New York, New York; for Defendants-Appellees.

OPINION

M. SMITH, Circuit Judge:

"WE WANT YOU BACK!" Many of us have received, through phone calls, emails, texts, and the post, the plaintive entreaties of companies with whom we have decided to cease doing business, seeking recommencement of our patronage. Such was the experience of James Andrews, who, after the dealership from which he bought a used car provided his personal information to Sirius XM Radio Inc. (Sirius XM), received unsolicited advertisements asking him to renew his radio subscription.

The primary question before us is whether Sirius XM's use of personal information derived from Andrews's driver's license violated the Driver's Privacy Protection Act of 1994 (DPPA), 18 U.S.C. §§ 2721–2725. Because we conclude that the DPPA does not apply where the source of personal information is a driver's license in the possession of its owner, rather than a state Department of Motor Vehicles (DMV), we affirm the district court's grant of summary judgment in favor of Sirius XM. We also affirm the district court's denial of Andrews's motion to amend his complaint

to add a claim under the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

FACTUAL AND PROCEDURAL BACKGROUND

I. Factual Background

On January 14, 2017, Andrews purchased a pre-owned 2012 Chevy Equinox from Auto Source, a small used car lot in Banning, California. He presented the dealership with his California driver's license, from which it obtained his name and PO Box address. He also filled out a California DMV Form 262—"Vehicle/Vessel Transfer and Reassignment Form"—a multipurpose form that serves as an odometer disclosure, bill of sale, and power of attorney. On the Form 262, Andrews provided his telephone number, street address, PO Box, and name. Auto Source input this information into its dealer management system (DMS), which ran on a database platform operated by a third party, AutoManager.

Andrews's Equinox came equipped with Sirius XM radio, a subscription-based satellite radio service. Gail Berger, Sirius XM's Vice President of Auto Remarketing, attested that her company has agreements with thousands of automotive dealerships across the country pursuant to which Sirius XM offers trial subscriptions for pre-owned vehicles and, in return, dealers provide Sirius XM with the names and addresses of customers who purchase or lease XM-equipped vehicles. According to Berger, Auto Source enrolled in Sirius XM's pre-owned program in 2015. The terms of the agreement provided that Sirius XM "requires the use of data that exists in [Auto Source's DMS], including customer data to activate [its] customers' SiriusXM Trial Service and to communicate with customers regarding their Trial Subscriptions and options to extend their SiriusXM services

following the Trial Subscriptions." It also permitted Auto Source's DMS provider, AutoManager, "to extract and share [its] DMS data with SiriusXM." A separate agreement between Sirius XM and AutoManager specified that this information included "Customer Data."

Berger stated that, following Andrews's purchase, AutoManager provided Sirius XM with a record of the sale. This electronic record included his name and street address. According to a Sirius XM manager, however, Andrews's PO Box was *not* provided by AutoManager; instead, Sirius XM obtained that information through a separate contractor that used the U.S. Postal Service's National Change of Address database. Andrews asserted that he gave neither Auto Source nor anyone else permission to share his personal information with Sirius XM.

Within days of Andrews's purchase, the deluge began. Sirius XM sent various letters to Andrews's PO Box between January and August 2017, imploring him—"We Want You Back!"—to resume his Sirius XM service after the subscription included with his car purchase ended. Sirius XM also telephoned him for the same purpose.

II. Procedural Background

On August 24, 2017, Andrews filed a putative class action complaint in the district court, alleging violations of the DPPA and seeking an injunction and statutory damages of $2,500 for each violation.

In his complaint, Andrews—apparently unaware of the agreements between Auto Source, AutoManager, and Sirius XM pursuant to which his personal information was shared—alleged that Sirius XM "obtained [his] name and address, as well as his phone number, from the motor vehicle

records, most likely the registration documents submitted to the DMV after he purchased the car." Prior to filing its motion for summary judgment, Sirius XM's counsel explained to Andrews's counsel that, contrary to Andrews's allegations, it had obtained his personal information not from the DMV, but instead from Auto Source and the Change of Address database. Subsequently, Andrews moved to file an amended complaint to add a claim for violation of the CFAA, based on Sirius XM's access to Auto Source's DMS.

The district court granted Sirius XM's motion for summary judgment, and denied Andrews's motion to file an amended complaint. As to the DPPA claim, the court determined, "[l]ike the Supreme Court and the vast majority of other courts to have analyzed the issue," that "the DPPA's definition of 'motor vehicle record' [] requir[es] that the DMV be the source of the 'record.'" Because the court found that Sirius XM obtained Andrews's personal information from his driver's license and the Form 262—neither of which, it determined, constituted a DMV record—it concluded that "the undisputed facts establish that [Sirius XM] did not 'use' 'personal information' 'from a motor vehicle record,'" and that Sirius XM was therefore entitled to summary judgment on the DPPA claim. Turning to Andrews's motion for leave to amend, the district court concluded that amendment would be futile because the proposed amended complaint "fail[ed] to allege that he ha[d] suffered a 'loss' or 'damage' cognizable under the CFAA."

This timely appeal followed.

JURISDICTION AND STANDARD OF REVIEW

We have jurisdiction pursuant to 28 U.S.C. § 1291. We review de novo a district court's grant of summary judgment.

WildEarth Guardians v. Provencio, 923 F.3d 655, 664 (9th Cir. 2019). "A court's denial of leave to amend is reviewed for an abuse of discretion." *Ebner v. Fresh, Inc.*, 838 F.3d 958, 963 (9th Cir. 2016).

ANALYSIS

I. DPPA

Andrews contends that the district court erred when it granted summary judgment in favor of Sirius XM, arguing that the company violated the DPPA's prohibition on using and disclosing personal information derived from DMV records when it obtained his name, address, and phone number from his driver's license and the Form 262. He urges us to "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's license] issued by a state DMV . . . the plaintiff can state a claim for violation of the DPPA." We decline to adopt such a holding, and instead conclude that Sirius XM's conduct fell outside the scope of the DPPA.

A. Origins and Scope of the DPPA

Congress enacted the DPPA in 1994, in response to a troubling phenomenon that occurred throughout the 1980s and early 1990s—state DMVs' practice of selling or freely disclosing drivers' personal information, which led to unfortunate consequences ranging from the trivial (onslaughts of random solicitations) to the tragic (the murders of several people by stalkers or ex-spouses). *See, e.g.*, 140 Cong. Rec. H2,518, H2,522–24 (daily ed. Apr. 20, 1994) (statement of Rep. Moran) ("In Iowa, a gang of thieves copied down the license plate numbers of expensive cars

they saw, found out the names and addresses of the owners and robbed their homes at night. In Virginia, a woman regularly wrote to the DMV, provided the license plate numbers of drivers and asked for the names and addresses of the owners who she claimed were stealing the fillings from her teeth at night."); 139 Cong. Rec. S15,745, S15,766 (daily ed. Nov. 16, 1993) (statement of Sen. Harkin) (recounting the story of a woman who visited an obstetrics clinics and received a "venomous letter" from anti-abortion activists who "got her name and address from department of transportation records, after they spotted her car parked near [the] clinic"); *Protecting Driver Privacy: Hearing on H.R. 3365 Before the Subcomm. on Civil & Constitutional Rights*, 1994 WL 212698 (Feb. 3, 1994) (statement of Rep. Moran) ("While the release of this information to direct marketers does not pose any inherent safety risks to people, it does present, to some people, an invasion of privacy.").[1] At that time, "[u]nder the law in over 30 States, it [was] permissible to give out to any person the name, telephone number, and address of any other person if a drivers' license or vehicle plate number [was] provided to a State agency." 139 Cong. Rec. at S15,765 (statement of Sen. Biden).

Accordingly, "[c]oncerned that personal information collected by States in the licensing of motor vehicle drivers was being released—even sold—with resulting loss of privacy for many persons, Congress provided federal

[1] Perhaps the most infamous victim of this practice was actress Rebecca Schaeffer, who was shot to death by an obsessed fan who hired a private investigator to find Schaeffer's home address, which the investigator then obtained from the DMV. *See* 140 Cong. Rec. at H2,522 (statement of Rep. Moran); *Protecting Driver Privacy: Hearing on H.R. 3365 Before the Subcomm. on Civil & Constitutional Rights*, 1994 WL 212822 (Feb. 3, 1994) (testimony of David Beatty, Dir. of Pub. Affairs, Nat'l Victim Ctr.).

statutory protection" through the DPPA. *Maracich v. Spears*, 570 U.S. 48, 51–52 (2013). As characterized by the Supreme Court, the purpose of the DPPA is to "regulate[] the disclosure and resale of personal information contained in the records of state DMVs." *Reno v. Condon*, 528 U.S. 141, 143 (2000); *see also id.* at 144 ("The DPPA establishes a regulatory scheme that restricts the States' ability to disclose a driver's personal information without the driver's consent."). Consistent with this primary objective, the first part of the DPPA expressly focuses on a state's own records. It prohibits "[a] State department of motor vehicles" from "knowingly disclos[ing] or otherwise mak[ing] available . . . personal information . . . about any individual obtained by the department in connection with a motor vehicle record." 18 U.S.C. § 2721(a).[2]

The DPPA's second part, by contrast, concerns not DMVs themselves, but instead those who illicitly seek information from motor vehicle records. Section 2722 makes it 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),"[3] and "for

[2] "'[P]ersonal information' means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status." 18 U.S.C. § 2725(3).

[3] Such permitted uses include "use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers." 18 U.S.C. § 2721(b). The statute also allows disclosure of an individual's personal information

any person to make false representation to obtain any personal information from an individual's motor vehicle record." *Id.* § 2722. It is this provision—along with the section that confers a private cause of action on those injured by violations of the statute, *id.* § 2724—on which Andrews relies to argue that Sirius XM's conduct violated the DPPA.

B. Andrews's Claim

To prevail on his DPPA claim, Andrews must satisfy § 2722(a) and prove that (1) Sirius XM knowingly obtained his personal information (2) from a motor vehicle record (3) for a nonpermissible use. *See Taylor v. Acxiom Corp.*, 612 F.3d 325, 335 (5th Cir. 2010). The first and third elements are undisputed here: Sirius XM obtained and used Andrews's name and telephone number—"personal information" as defined by the DPPA—for nonpermissible promotional purposes. *See* 18 U.S.C. §§ 2721(b), 2725(3). Accordingly, the key issue on appeal is whether the documents from which Sirius XM obtained Andrews's personal information—specifically, his driver's license and the Form 262—qualify as "motor vehicle records" pursuant to the statute. We conclude that they do not.

The DPPA defines a "motor vehicle record" 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." *Id.* § 2725(1). Sirius XM argues that "a driver's

"[f]or use in the normal course of business by a legitimate business," but only "to verify the accuracy of personal information submitted by the individual" and, "if such information as so submitted is not correct or is no longer correct, to obtain the correct information" in limited circumstances. *Id.* § 2721(b)(3).

license cannot qualify under that definition," citing to the district court's analysis:

> [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 [Andrews] 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 [it] also be a "record."

We are not wholly persuaded by this linguistic analysis of the DPPA. Sirius XM argues, as the district court concluded, that "construing a 'motor vehicle record' to include a driver license would render the definition's use of both 'record' and 'pertains to' as surplusage," but a "record" is defined as, among other things, "[i]nformation that is inscribed on a tangible medium." *Record*, *Black's Law Dictionary* (11th ed. 2019); *see also Webster's Third New International Dictionary* 1,898 (2002) (defining "record" as "evidence, knowledge, or information remaining in permanent form (as a relic, inscription, document)"). A driver's license is a tangible document that serves as proof of an individual's permission to operate a motor vehicle, and can therefore be considered a "record." And, although Sirius XM raises a fair point as to whether "pertains to" would be

rendered surplusage, it would make little practical sense that a photocopy of a driver's license—which is indisputably a "record that pertains to a motor vehicle operator's permit"—could be a qualifying motor vehicle record, but the actual license lying right next to it on the desk at the DMV, containing identical personal information, could not. We are therefore unconvinced that a driver's license is not a "record" based solely on the wording of the statute's definition.

But just because a driver's license is a "record" does not necessarily mean it is a "*motor vehicle* record." Reading § 2722's words "in their context and with a view to their place in the overall statutory scheme," *Davis v. Mich. Dep't of Treasury*, 489 U.S. 803, 809 (1989), we conclude that a driver's license in the possession of its owner is not a qualifying "motor vehicle record" under the DPPA.

It is clear, from the legislative history and case law, that Congress was motivated to enact the DPPA by the "growing threat from stalkers and criminals who could acquire personal information *from state DMVs*," as well as "*the States'* common practice of selling personal information to businesses engaged in direct marketing and solicitation." *Maracich*, 570 U.S. at 57 (emphases added). With this purpose in mind, we interpret § 2721—prohibiting DMVs from "knowingly disclos[ing] . . . personal information," 18 U.S.C. § 2721(a)—as covering one side of the prohibited transaction. Section 2722, by contrast, covers the *other* side of that same transaction, by creating liability for the person who "obtain[s] or disclose[s] personal information" from the DMV's records. *Id.* § 2722(a).

A driver's license, though issued by the DMV, becomes the possession of *an individual*, not the DMV that issued it.[4] Congress intended the DPPA to reflect the Privacy Act of 1974, *see Protecting Driver Privacy*, 1994 WL 212698 (statement of Rep. Moran) ("The bill incorporates [] the intent of the 1974 Privacy Act."), which defines a "record" as "information about an individual *that is maintained by an agency*." 5 U.S.C. § 552a(a)(4) (emphasis added); *see also Wilborn v. Dep't of Health & Human Servs.*, 49 F.3d 597, 600 (9th Cir. 1995) ("[I]f a party discloses information obtained independently of any records, such a disclosure does not violate the [Privacy] Act, even if identical information is contained in the records."), *abrogated on other grounds by Doe v. Chao*, 540 U.S. 614 (2004). A driver's license in the possession of its owner is no longer maintained by the DMV, and so such a record is outside the bounds of the DPPA. The same is true of the Form 262 at issue here, which did not even pass through the DMV before the information made its way to Sirius XM.

Put another way, we conclude that where, as here, the initial source of personal information is a record in the possession of an individual, rather than a state DMV, then use or disclosure of that information does not violate the DPPA. This conception of the DPPA's scope is consistent both with its clear purpose, *see Maracich*, 570 U.S. at 51–52 (noting Congress's specific concern with the release of personal information *by States*), and with two other circuits

[4] After all, a Good Samaritan who finds a driver's license lying on the sidewalk would probably return it to the person to whom it was issued, not to the DMV that issued it.

that have previously interpreted the statute, albeit in unpublished opinions.[5]

Andrews contends that Sirius XM's conduct violated the literal text of the statute. But, even if the statute could be read to cover this conduct, we will not adopt "a literal interpretation [that] 'would thwart the purpose of the overall statutory scheme or lead to an absurd result.'" *Wilshire Westwood Assocs. v. Atl. Richfield Corp.*, 881 F.2d 801, 804 (9th Cir. 1989) (quoting *Brooks v. Donovan*, 699 F.2d 1010, 1011 (9th Cir. 1983)); *see also Nixon v. Mo. Mun. League*, 541 U.S. 125, 138 (2004). As discussed above, Andrews's expansive conception of the DPPA does not align with the statute's clear purpose. And, although both Andrews and Sirius XM utilized a considerable quantity of briefing ink trading hypotheticals and parading various horribles in support of their respective positions, we conclude that Andrews's position yields the more absurd results.

It would be patently unreasonable, for example, to penalize a security guard's use of a driver's license photograph—"personal information" under the DPPA, 18 U.S.C. § 2725(3)—on temporary security badges in

[5] *See Fontanez v. Skepple*, 563 F. App'x 847, 848–49 (2d Cir. 2014) ("[T]he DPPA does not protect against the use of personal information obtained from a driver's license provided by the holder as proof of identity to gain access to a facility. . . . [T]he statute was intended to bar the State from disclosing personal information obtained from DMV records without the individual's consent."); *Siegler v. Best Buy Co. of Minn.*, 519 F. App'x 604, 605 (11th Cir. 2013) ("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 [] records. . . . On its face, the Act is concerned only with information disclosed, in the first instance, by state DMVs." (footnote omitted)).

office buildings and other locations.[6] After all, "[t]he 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.*, 726 F.3d 42, 50 (2d Cir. 2013) (second alteration in original) (quoting 140 Cong. Rec. at H2,522 (statement of Rep. Moran)). In light of this practical mindset, we will not subject a range of commonplace and innocuous activities involving driver's licenses to potential DPPA liability.[7] Accordingly, given that the statute was clearly intended to prevent the unauthorized, nonconsensual, and involuntary disclosure of personal information from

[6] For that matter, it would be absurd to prosecute the Good Samaritan referenced in footnote 4, *supra*—a possibility under Andrews's conception of the statute, given that returning a lost license to its owner is not an enumerated permissible use under the DPPA. *See* 18 U.S.C. § 2721(b).

[7] The district court in *Whitaker v. Appriss, Inc.* provided further analysis on this point, noting that "[s]trange and far-reaching results follow from . . . treating the license as the 'motor vehicle record.'" 266 F. Supp. 3d 1103, 1109 (N.D. Ind. 2017). It continued,

> Any non-excepted use of information pulled off a driver's license provided by its holder would subject the user of that information to DPPA liability. . . . For example, a person who uses information on her spouse's driver's license information to make an order or reservation would be liable to the spouse for a DPPA violation. . . . These interpretations balloon liability beyond the Act's purpose of preventing disclosures by DMVs and misuse of information disclosed to third parties from DMVs.

Id. at 1109–10.

DMV records, we conclude that Andrews's driver's license was not a "motor vehicle record" pursuant to the DPPA.

We acknowledge the potential abuses—such as the intrusive behavior Andrews experienced in this case—that can result from exploitation of personal information contained on an individual's driver's license. But we ultimately agree with the conclusion of the district court in *O'Brien v. Quad Six, Inc.*, which considered the use of a plaintiff's personal information after he presented his driver's license as identification at a nightclub:

> We are sympathetic to plaintiff's concerns about the way businesses collect and use personal information, and its implications for all of our privacies. But that is not what Congress intended the DPPA to regulate. This statute seeks to control dissemination of information collected using the coercive power of the state. It does not regulate information freely given by consumers to private businesses, such as when plaintiff tendered his driver's license to [the nightclub].

219 F. Supp. 2d 933, 934–35 (N.D. Ill. 2002). Aggrieved plaintiffs, Andrews included, might have other statutory remedies to rectify alleged abuses of their personal information. But the DPPA—a statute concerned solely with the actions of state DMVs and those who illicitly retrieve information from them—is not the proper vehicle

for such redress, where, as here, the source of that information is a driver's license in its owner's possession.[8]

* * *

Sirius XM correctly observes that "[t]he DPPA was not designed to remedy every misuse of personal information that happened to come from a driver's license." Instead, its scope is limited to impermissible disclosures by state DMVs to those who seek information from them. Andrews concedes that neither Sirius XM nor anyone else requested or acquired his information from the California DMV. Therefore, we conclude that Sirius XM's conduct, annoying as it might have been, did not violate the DPPA.

II. CFAA

Andrews also challenges the district court's conclusion that amending his complaint to add a claim under the CFAA would have been futile.

The CFAA makes it unlawful to, among other things, "intentionally access[] a computer without authorization" and obtain "information from any protected computer." 18 U.S.C. § 1030(a)(2). It provides a private right of action for "[a]ny person who suffers damage or loss by reason of a violation of [the statute] . . . against the violator to obtain compensatory damages and injunctive relief or other equitable relief," but "only if the conduct involves 1 of the factors set forth" elsewhere in the CFAA. *Id.* § 1030(g). Of the five possible factors, the only one relevant to Andrews's potential claim is that the offense caused "loss to 1 or more

[8] We similarly conclude that the Form 262—which was neither produced nor maintained by the DMV—does not constitute a "motor vehicle record" for purposes of the DPPA.

persons during any 1-year period . . . aggregating at least $5,000 in value." *Id.* § 1030(c)(4)(A)(i)(I). As Sirius XM correctly characterizes the situation, "[w]hether Andrews could have brought a viable CFAA claim turns on whether Andrews could plausibly allege a qualifying loss."

Andrews's theory of loss is that he and his fellow class members were denied the profits they might have received from commodifying the personal information that Sirius XM allegedly obtained through unlawful means. His proposed amended complaint claimed that this information

> was extremely valuable . . . . This information is what is called in the marketing industry a "hot lead." [Andrews] is informed and believes, and thereupon alleges, that the retail value of a "hot lead" of this nature and for the price point of [Sirius XM's] subscription plans is at least $100.

Accordingly, because Sirius XM allegedly "stole the personal information without compensating [Andrews], he lost the value of that information and the opportunity to sell it."[9]

The CFAA, however, defines "loss" as "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

[9] The proposed amended complaint pleaded that Sirius XM "obtained the aforementioned valuable personal information belonging to at least 100 persons," and that therefore his claim satisfied the CFAA's $5,000 threshold.

consequential damages incurred because of interruption of service." *Id.* § 1030(e)(11). This is a narrow conception of "loss," and the definition does not include a provision that aligns with Andrews's theory.

"[I]t is a commonplace of statutory construction that the specific governs the general." *Morales v. Trans World Airlines, Inc.*, 504 U.S. 374, 384 (1992). This "canon has full application . . . to statutes such as the one here, in which a general authorization and a more limited, specific authorization exist side-by-side." *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 566 U.S. 639, 645 (2012). In such cases, "[t]he terms of the specific authorization must be complied with," to avoid "the superfluity of a specific provision that is swallowed by the general one." *Id.* Accordingly, any theory of loss must conform to the limited parameters of the CFAA's definition. And although the definition does include "revenue lost," that refers *only* to losses that occurred "because of interruption of service." 18 U.S.C. § 1030(e)(11); *see also Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC*, 774 F.3d 1065, 1073–74 (6th Cir. 2014) ("[T]he plain language of the [CFAA] treats lost revenue as a different concept from incurred costs, and permits recovery of the former only where connected to an 'interruption in service.'" (alterations in original) (quoting *Nexans Wires S.A. v. Sark-USA, Inc.*, 166 F. App'x 559, 562 (2d Cir. 2006))). Andrews does not—and cannot—argue that his allegedly lost revenue occurred because of an interruption of service, and so his purported injury is not cognizable under the CFAA.

We further observe that the CFAA is "an anti-hacking statute," not "an expansive misappropriation statute." *United States v. Nosal*, 676 F.3d 854, 857 (9th Cir. 2012) (en banc). The statute's "loss" definition—with its references to

damage assessments, data restoration, and interruption of service—clearly limits its focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself. Given this circumscribed focus, and the principle that "a general statutory term should be understood in light of the specific terms that surround it," *Hughey v. United States*, 495 U.S. 411, 419 (1990), we will not expand the CFAA's limited conception of loss to include the sort of injury pleaded in Andrews's proposed amended complaint.[10]

Accordingly, the district court did not abuse its discretion when it concluded that an amendment adding a CFAA claim to Andrews's complaint would have been futile.

CONCLUSION

The legislative history of the DPPA, and the decisions of the Supreme Court interpreting it, demonstrate that the purpose of the statute was to prevent the acquisition and exploitation of personal information from the records of state DMVs. We therefore conclude that Sirius XM did not violate the DPPA when it used personal information obtained from Andrews's driver's license. We further

[10] Andrews argues that this is "a hyper-technical interpretation of 'loss'" that is contrary to our decision in *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930 (9th Cir. 2004). That case, however, does not support Andrews's expansive interpretation of "loss." Although *Creative Computing* did indicate that "loss of business and business goodwill" constitutes "economic damages" within the meaning of the CFAA, *id.* at 935, it did so when considering the scope of recoverable damages, *see* 18 U.S.C. § 1030(g), *not* what qualifies as a predicate "loss." Whether or not a lost business opportunity can be recovered as economic damages is a different question than whether it constitutes a loss that gives rise to a civil CFAA action in the first place. Therefore, our conclusion is not inconsistent with *Creative Computing*.

conclude that, given the CFAA's limited conception of loss, the district court did not abuse its discretion when it denied Andrews leave to amend on futility grounds.

AFFIRMED.

United States Court of Appeals for the Ninth Circuit

Office of the Clerk
95 Seventh Street
San Francisco, CA 94103

Information Regarding Judgment and Post-Judgment Proceedings

Judgment

- This Court has filed and entered the attached judgment in your case. Fed. R. App. P. 36. Please note the filed date on the attached decision because all of the dates described below run from that date, not from the date you receive this notice.

Mandate (Fed. R. App. P. 41; 9th Cir. R. 41-1 & -2)

- The mandate will issue 7 days after the expiration of the time for filing a petition for rehearing or 7 days from the denial of a petition for rehearing, unless the Court directs otherwise. To file a motion to stay the mandate, file it electronically via the appellate ECF system or, if you are a pro se litigant or an attorney with an exemption from using appellate ECF, file one original motion on paper.

Petition for Panel Rehearing (Fed. R. App. P. 40; 9th Cir. R. 40-1)
Petition for Rehearing En Banc (Fed. R. App. P. 35; 9th Cir. R. 35-1 to -3)

(1) A. Purpose (Panel Rehearing):

- A party should seek panel rehearing only if one or more of the following grounds exist:
  - ► A material point of fact or law was overlooked in the decision;
  - ► A change in the law occurred after the case was submitted which appears to have been overlooked by the panel; or
  - ► An apparent conflict with another decision of the Court was not addressed in the opinion.
- Do not file a petition for panel rehearing merely to reargue the case.

B. Purpose (Rehearing En Banc)

- A party should seek en banc rehearing only if one or more of the following grounds exist:

- ► Consideration by the full Court is necessary to secure or maintain uniformity of the Court's decisions; or
- ► The proceeding involves a question of exceptional importance; or
- ► The opinion directly conflicts with an existing opinion by another court of appeals or the Supreme Court and substantially affects a rule of national application in which there is an overriding need for national uniformity.

(2) Deadlines for Filing:

- A petition for rehearing may be filed within 14 days after entry of judgment. Fed. R. App. P. 40(a)(1).
- If the United States or an agency or officer thereof is a party in a civil case, the time for filing a petition for rehearing is 45 days after entry of judgment. Fed. R. App. P. 40(a)(1).
- If the mandate has issued, the petition for rehearing should be accompanied by a motion to recall the mandate.
- *See* Advisory Note to 9th Cir. R. 40-1 (petitions must be received on the due date).
- An order to publish a previously unpublished memorandum disposition extends the time to file a petition for rehearing to 14 days after the date of the order of publication or, in all civil cases in which the United States or an agency or officer thereof is a party, 45 days after the date of the order of publication. 9th Cir. R. 40-2.

(3) Statement of Counsel

- A petition should contain an introduction stating that, in counsel's judgment, one or more of the situations described in the "purpose" section above exist. The points to be raised must be stated clearly.

(4) Form & Number of Copies (9th Cir. R. 40-1; Fed. R. App. P. 32(c)(2))

- The petition shall not exceed 15 pages unless it complies with the alternative length limitations of 4,200 words or 390 lines of text.
- The petition must be accompanied by a copy of the panel's decision being challenged.
- An answer, when ordered by the Court, shall comply with the same length limitations as the petition.
- If a pro se litigant elects to file a form brief pursuant to Circuit Rule 28-1, a petition for panel rehearing or for rehearing en banc need not comply with Fed. R. App. P. 32.

- The petition or answer must be accompanied by a Certificate of Compliance found at Form 11, available on our website at www.ca9.uscourts.gov under *Forms.*
- You may file a petition electronically via the appellate ECF system. No paper copies are required unless the Court orders otherwise. If you are a pro se litigant or an attorney exempted from using the appellate ECF system, file one original petition on paper. No additional paper copies are required unless the Court orders otherwise.

Bill of Costs (Fed. R. App. P. 39, 9th Cir. R. 39-1)

- The Bill of Costs must be filed within 14 days after entry of judgment.
- See Form 10 for additional information, available on our website at www.ca9.uscourts.gov under *Forms.*

Attorneys Fees

- Ninth Circuit Rule 39-1 describes the content and due dates for attorneys fees applications.
- All relevant forms are available on our website at www.ca9.uscourts.gov under *Forms* or by telephoning (415) 355-7806.

Petition for a Writ of Certiorari

- Please refer to the Rules of the United States Supreme Court at www.supremecourt.gov

Counsel Listing in Published Opinions

- Please check counsel listing on the attached decision.
- If there are any errors in a published opinion, please send a letter **in writing within 10 days** to:
  - ► Thomson Reuters; 610 Opperman Drive; PO Box 64526; Eagan, MN 55123 (Attn: Jean Green, Senior Publications Coordinator);
  - ► and electronically file a copy of the letter via the appellate ECF system by using "File Correspondence to Court," or if you are an attorney exempted from using the appellate ECF system, mail the Court one copy of the letter.

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 10. Bill of Costs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form10instructions.pdf

9th Cir. Case Number(s)

Case Name

The Clerk is requested to award costs to (*party name(s)*):

I swear under penalty of perjury that the copies for which costs are requested were actually and necessarily produced, and that the requested costs were actually expended.

Signature **Date**

*(use "*s/[typed name]*" to sign electronically-filed documents)*

COST TAXABLE	**REQUESTED** *(each column must be completed)*			
DOCUMENTS / FEE PAID	No. of Copies	Pages per Copy	Cost per Page	TOTAL COST
Excerpts of Record*			$	$
Principal Brief(s) *(Opening Brief; Answering Brief; 1st, 2nd , and/or 3rd Brief on Cross-Appeal; Intervenor Brief)*			$	$
Reply Brief / Cross-Appeal Reply Brief			$	$
Supplemental Brief(s)			$	$
Petition for Review Docket Fee / Petition for Writ of Mandamus Docket Fee				$
			TOTAL:	$

***Example:** Calculate 4 copies of 3 volumes of excerpts of record that total 500 pages [Vol. 1 (10 pgs.) + Vol. 2 (250 pgs.) + Vol. 3 (240 pgs.)] as:*
No. of Copies: 4; Pages per Copy: 500; Cost per Page: $.10 (or actual cost IF less than $.10);
TOTAL: 4 x 500 x $.10 = $200.

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov