

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

BRIAN FELSEN, MATTHEW	:	CIVIL ACTION
RAGUSANO, <i>individually and on behalf</i>	:	
<i>of all others similarly situated</i>	:	
	:	
v.	:	NO. 25-2359
	:	
THE VANGUARD GROUP, INC.	:	

MEMORANDUM

MURPHY, J.

September 15, 2026

These days, most everyone is accustomed to handling their personal affairs online through websites or apps. And it is natural to expect that service providers will protect from disclosure our medical records, financial transactions, and other sensitive information. Perceived failures lead to lawsuits, but it is not always easy to find the correct legal framework to govern the dispute. And it is not a safe assumption that any violation of a statute allows a plaintiff to pursue relief in federal court. In this case, plaintiffs say that financial-services provider Vanguard allowed third parties like Google to see the financial products that plaintiffs searched for, bought, and sold on Vanguard's platform. According to plaintiffs, Vanguard's actions violated the Federal Wiretap Act, Pennsylvania and California's statutory analogs, and the California Constitution and common law. Following the path well trod by defendants in analogous cases, Vanguard moves to dismiss, arguing that the disclosure of plaintiffs' activity on Vanguard's platform caused plaintiffs no concrete harm, so they lack Article III standing. Vanguard further argues that the complaint fails to state a claim under federal or state law. For the reasons explained below, we hold that plaintiffs have standing. But considering the sufficiency of the pleadings, we dismiss without prejudice the Federal Wiretap Act claims as well as plaintiffs' California common law and constitutional claims.

I. Factual Allegations

Vanguard Group, Inc. is a financial services company that provides online brokerage accounts through a website and mobile application. DI 12 ¶ 13.¹ Plaintiffs Brian Felsen, Matthew Ragusano, and Nambaramey Dy are accountholders who use Vanguard’s website or app to buy and sell securities and other financial products. *Id.* ¶¶ 6-8. They bring this action on behalf of themselves and a class of Vanguard accountholders, alleging that Vanguard unlawfully “discloses and assists several third parties . . . in intentionally intercepting” communications between plaintiffs and Vanguard through its website or app. *Id.* ¶ 3.

Specifically, plaintiffs allege that Vanguard’s brokerage website and app contained code that allowed the LinkedIn Corporation, Google LLC, and Meta Platforms, Inc. to obtain information about plaintiffs’ investment activities. DI 12 ¶¶ 3, 5, 80. This information included the stocks that plaintiffs searched for, bought, and sold. *Id.* ¶ 87. These third parties then used that information for “marketing purposes,” which allowed Vanguard to advertise more effectively and the third parties to improve their own advertising services. *Id.* ¶¶ 94-96, 99-101, 104-06.

The method of alleged interception and the contents of the communications allegedly intercepted are broadly similar for LinkedIn, Google, and Meta — all involve Vanguard allowing these third parties to embed pieces of code on Vanguard’s website and app that allowed the third parties to see what users were doing on Vanguard’s website or app. For LinkedIn, plaintiffs allege that a piece of code called a “LinkedIn Insight Tag” “was embedded on” Vanguard’s website and app. DI 12 ¶ 48. The LinkedIn Insight tag allowed LinkedIn to

¹ We use the sequential pagination supplied by the CM/ECF docketing system.

intercept and record users’ “personal information from account creation, the type of account opened, queries in the search box, ticker symbol, and action taken along with an identifier used to track the visitor’s identity across websites.” *Id.* at ¶ 48. As to Google, plaintiffs allege that “the Google Analytics tracking code” was “employed on” Vanguard’s website and app. *Id.* ¶ 65. This code allowed Google to collect broadly similar information. *Id.* ¶ 64. Finally, with respect to Meta, plaintiffs allege that “the Meta Pixel” was “employed on” Vanguard’s website and app. *Id.* ¶ 79. The Meta Pixel likewise captured information about users’ account creation and stock purchases. *Id.* at ¶¶ 85-87.

Plaintiffs’ operative complaint asserts claims under the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*, DI 12 ¶¶ 121-43; Pennsylvania’s Wiretapping and Electronic Surveillance Control Act (WESCA), 18 Pa. Cons. Stat. § 5701, *et seq.*, DI 12 ¶¶ 144-55; the California Invasion of Privacy Act (CIPA), Cal. Penal Code §§ 631 & 632, DI 12 ¶¶ 156-79; and the California Constitution and common-law right to privacy, *id.* ¶¶ 180-86. The Federal Wiretap Act claim is brought by all three plaintiffs on behalf of themselves and a nationwide class. *Id.* ¶ 121. Plaintiff Dy, a Pennsylvania citizen, brings the Pennsylvania WESCA claim on behalf of himself and a Pennsylvania subclass. *Id.* ¶ 144. Plaintiffs Felsen and Ragusano, both California citizens, bring the California claims on behalf of themselves and a California subclass. *Id.* ¶¶ 156, 169, 180.

II. Vanguard’s Motion to Dismiss

Following Vanguard’s motion to dismiss (DI 10) plaintiffs’ original complaint (DI 1), plaintiffs filed a first amended complaint (DI 12). We then denied Vanguard’s original motion to dismiss as moot. DI 16. Vanguard now moves to dismiss plaintiffs’ amended complaint in

whole on two grounds. DI 13-1. First, Vanguard moves to dismiss for lack of subject matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1), arguing that plaintiffs lack Article III standing. *Id.* at 12-15. Vanguard argues that plaintiffs’ alleged injury is insufficiently concrete to give rise to a case or controversy under Article III, so we lack jurisdiction. *Id.* Second, Vanguard moves to dismiss under Federal Rule of Civil Procedure 12(b)(6), arguing that plaintiffs’ amended complaint fails to state a claim. *Id.* at 15-32. Vanguard raises numerous arguments in favor of dismissal under Rule 12(b)(6), which we explore in more detail below.

III. Legal Standards

Under Rule 12(b)(1), we must grant a motion to dismiss if we lack subject-matter jurisdiction over a claim. If the plaintiff lacks Article III standing, we lack subject-matter jurisdiction. *Ballentine v. United States*, 486 F.3d 806, 810 (3d Cir. 2007). At the motion to dismiss stage, we assess standing by “apply[ing] the same standard of review we use when assessing a motion to dismiss for failure to state a claim.” *Finkelman v. Nat’l Football League*, 810 F.3d 187, 194 (3d Cir. 2016) (citing *In re Schering Plough Corp. Intron/Temodar Consumer Class Action*, 678 F.3d 235, 243 (3d Cir.2012)). A plaintiff can thus survive a motion to dismiss for lack of standing where — putting aside any conclusory allegations — the complaint “allege[s] facts that affirmatively and plausibly suggest that [they] ha[ve] standing to sue.” *Id.* (quoting *Amidax Trading Grp. v. S.W.I.F.T. SCRL*, 671 F.3d 140, 145 (2d Cir. 2011)).

The motion to dismiss standard of review under Federal Rule of Civil Procedure 12(b)(6) is the same, *Finkelman*, 810 F.3d at 194, but we analyze whether the facts alleged plausibly satisfy the elements of the cause of action rather than the elements of standing, *see Ashcroft v.*

Iqbal, 556 U.S. 662, 678 (2009). We draw reasonable inferences in the plaintiffs’ favor. *Iqbal*, 556 U.S. at 678. Mere legal conclusions or threadbare recitals of the elements of a cause of action will not suffice. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007).

IV. Analysis

A. Article III Standing

Article III of the Constitution “confines the federal judicial power to the resolution of ‘Cases’ and ‘Controversies.’” *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021). “For there to be a case or controversy under Article III, the plaintiff must have a personal stake in the case — in other words, standing.” *Id.* (citation modified). This requires the plaintiff to show: (1) an injury-in-fact that is (2) fairly traceable to the defendant’s alleged conduct, and (3) redressable by a favorable judicial decision. *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). Only the first element of standing — injury in fact — is contested here. An injury-in-fact requires a plaintiff’s suffering “an invasion of a legally protected interest” that is “concrete and particularized,” as well as “actual or imminent, not conjectural or hypothetical.” *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (citation modified).

Here, Vanguard argues that the plaintiffs’ injuries were not sufficiently concrete. We disagree. While “[t]he ‘most obvious’ concrete injuries result from ‘traditional tangible harms, such as physical harms and monetary harms,’” intangible harms can also be concrete. *In re BPS Direct, LLC; Cabela’s, LLC Wiretapping Litig.*, 175 F.4th 423, 429 (3d Cir. 2026) (quoting *TransUnion*, 594 U.S. at 425). Specifically, those “injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts” are concrete injuries. *TransUnion*, 594 U.S. at 425. So where, as here, “plaintiffs allege an intangible harm,

we ask whether they have identified a close historical or common-law analogue for their asserted injury. We do so by comparing the kind of harm a plaintiff alleges with the kind of harm caused by a comparator tort at common law.” *BPS Direct*, 175 F.4th at 429 (citation modified).

In this case, plaintiffs’ comparator tort is intrusion upon seclusion. DI 22 at 5-6; *see* DI 19 at 10. In the communications-interception context, the kind of harm that tort seeks to protect against is the dissemination of a communication that the plaintiff would have reasonably expected to remain private. *See Santoro v. Tower Health*, — F.4th —, No. 24-3173, 2026 WL 2543842, at *4 (3d Cir. Aug. 28, 2026), *DeLong v. PHE, Inc.*, No. CV 24-5212, 2025 WL 2447787, at *5 (E.D. Pa. Aug. 25, 2025). A plaintiff can show that he reasonably expected a communication to remain private in at least two ways. First, he can show a communication contains the kind of “personal and sensitive” information that one would expect not to be disseminated, at least absent consent. *BPS Direct*, 175 F.4th at 431; *see Santoro*, — F.4th —, 2026 WL 2543842, at *4. Second, he can show that the recipient of the communication expressly represented that it would remain private. *See In re: Google Inc. Cookie Placement Consumer Priv. Litig.*, 934 F.3d 316, 324-25 (3d Cir. 2019) (“Google Inc. Cookie Placement II”); *DeLong*, 2025 WL 2447787, at *5. Here, plaintiffs have plausibly alleged that their communications fit into the former category.²

In finding that the communications at issue contained personal and sensitive information, we are guided by the Third Circuit’s decision in *BPS Direct*, 175 F.4th 423. There, plaintiffs alleged that an online retailer allowed third parties to intercept their complete credit and debit

² Because plaintiffs have plausibly alleged the interception of “personal and sensitive” information, we decline to address their argument that Vanguard’s representation that “[t]his application is secure” amounted to an express representation that information entered into the app would remain private. DI 19 at 11-12.

card information. *Id.* at 427-28, 431. The court held that because such information was “rightly viewed as highly sensitive,” “one expects” it “to be free from prying eyes.” *Id.* at 433. The information’s interception thus “caused th[e] plaintiffs harm closely analogous to that vindicated by the intrusion upon seclusion tort.” *Id.* In reaching this holding, the court noted that “the contents of [the plaintiff’s] wallet or bank” would also be a type of information that the intrusion upon seclusion tort protects from disclosure, suggesting that financial information is a type of personal and sensitive information. *See id.*; *see also In re Boston Herald, Inc.*, 321 F.3d 174, 190 (1st Cir. 2003) (“Personal financial information, such as one’s income or bank account balance, is universally presumed to be private, not public.”); *Halman Aldubi Provident & Pension Funds Ltd. v. Teva Pharms. Indus. Ltd.*, No. CV 20-4660, 2023 WL 1100995, at *4 (E.D. Pa. Jan. 30, 2023) (similar).

Turning to plaintiffs’ complaint with this guidance in mind, we think it plausibly alleges that the intercepted communications contained personal and sensitive information. Like the “contents of [a plaintiff’s] wallet or bank,” *BPS Direct*, 175 F.4th at 433, information pertaining to the financial products that plaintiffs buy, sell, or search for on Vanguard’s website or app is a type of personal financial information. Plaintiffs allege that the intercepted communications contained this kind of information — specifically, they allege that LinkedIn, Google, and Meta “intercept each stage of a user’s selection of Domestic Stock for investment, the ticker name, and the action the user is taking with this investment.” DI 12 ¶ 87. Thus, plaintiffs plausibly allege an injury analogous to that protected by the intrusion upon seclusion tort.

Vanguard also argues that plaintiffs’ allegations are not sufficiently specific because they rely on how third parties intercept communications on Vanguard’s website and app generally,

rather than alleging which specific communications were intercepted. DI 13-1 at 15-16. But plaintiffs allege that they held accounts with Vanguard and used its website or app to search for and purchase financial products. DI 12 at ¶¶ 6-8. They further allege that the website and app allowed third parties to intercept information about users' searches for and trades of financial products. *Id.* at ¶ 87. While plaintiffs do not allege the specific trades of theirs at issue, *id.* at 3 n.1, it is at least plausible, drawing reasonable inferences in their favor, that plaintiffs' searches and trades were intercepted by the technologies employed with respect to all users. No more specificity is required to establish standing at the pleading stage. *See Santoro*, — F.4th —, 2026 WL 2543842, at *4 (rejecting the argument that “[p]laintiffs needed to identify the specific information” allegedly disseminated where that information was identified as “individually-identifiable health information” in general terms).

Vanguard also argues that the Third Circuit's decision in *Cook*, 148 F.4th 153, undermines standing. DI 23 at 2-3. There, the Third Circuit held that information about a plaintiff's browsing activity on GameStop's retail website was not “sensitive or personal.” *Cook*, 148 F.4th at 159. This Court reached a similar conclusion for a different kind of retail product in *Delong*, 2025 WL 2447787, at *7. This case, however, is distinguishable in that plaintiffs were not merely viewing retail products but also engaging in online activity that revealed *financial* information, a category of information traditionally recognized as sensitive. *See supra*; *see also Stevens v. TD Bank, N.A.*, No. CV 24-8311, 2026 WL 1878514, at *5 (D.N.J. June 30, 2026) (distinguishing from *Cook* where the browsing activity at issue involved researching financial products). This case is further distinguishable from *Cook* because in that case “plaintiff did not allege that GameStop identified her.” 148 F.4th at 160. Here, by contrast,

plaintiffs allege that they shared “personally identifying information, including their name and email address” with Vanguard, DI 12 ¶ 2. Further, drawing reasonable inferences in their favor, plaintiffs plausibly allege that LinkedIn, Google, and Meta could identify plaintiffs and associate the intercepted information with them. *See id.* ¶¶ 48-49, 64, 72-73.

B. Federal Wiretap Act

To plead a prima facie case under the Federal Wiretap Act, a plaintiff must allege that the defendant “(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device.” *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 274 (3d Cir. 2016). The Act is a one-party consent statute, so “ordinarily, no cause of action will lie against a private person ‘where such person is a party to the communication’” *See In re: Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 135 (3d Cir. 2015) (“Google Inc. Cookie Placement I”) (quoting 18 U.S.C. § 2511(2)(d)). But when the “communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State,” a party to the communication may be held liable. *Id.* at 135 n.22 (quoting 18 U.S.C. § 2511(2)(d)).

It is undisputed that Vanguard was a party to the relevant communications, so plaintiffs’ Wiretap Act claim fails unless plaintiffs can show the interception was for the purpose of committing a crime or tort. Such a crime or tort cannot be “the alleged wiretapping itself” but rather must be “acts secondary to the acquisition of the communication involving tortious or criminal use of the interception’s fruits.” *Google Inc. Cookie Placement I*, 806 F.3d at 145. So

here, plaintiffs must show that the financial information that was allegedly intercepted was used for a criminal or tortious act “independent” of the interception. *See id.*

Plaintiffs argue that their complaint “clearly sets forth the crimes and torts committed against Plaintiffs, including violations of CIPA, WESCA, the California Constitution, the [Gramm-Leach-Bliley Act], and intrusion upon seclusion.” DI 19 at 17 (citing DI 12 ¶¶ 25-26, 85-92, 144-186). But plaintiffs offer no explanation as to how these torts and crimes are *independent* of the interception, and their cited allegations — to the extent they allege tortious or criminal conduct at all — focus on the acts of interception. Plaintiffs also point to “additional privacy violations” that “occurred after the interception, when the data collected was assembled into profiles by the Third Parties and used to target Plaintiffs with advertising, which ‘[was] done for the purpose of improperly increasing its own advertising efficiency, as well as Google’s [LinkedIn’s, and Meta’s].’” *Id.* (citing DI 12 ¶ 102; ¶¶ 93-101). But plaintiffs do not explain how this collection and assembly amounted to a crime or tort, and we decline to fill that gap on their behalf. *See Hausknecht v. John Hancock Life Ins. Co. of New York*, 614 F. Supp. 3d 168, 186 (E.D. Pa. 2022) (“[T]his Court’s role is not to craft arguments for the parties, especially those represented by counsel.”). Finally, plaintiffs also gesture at an argument that the tortious or criminal act need not be independent of the interception. DI 19 at 17-19. But plaintiffs cite no binding authority for this argument, and it is directly contradicted by binding Third Circuit precedent. *Google Inc. Cookie Placement I*, 806 F.3d at 145.

C. Pennsylvania Wiretapping and Electronic Surveillance Control Act

Pennsylvania’s state law analog to the Federal Wiretap Act — WESCA — provides a cause of action to “any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of that statute” against “any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication.” *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121, 125 (3d Cir. 2022) (quoting 18 Pa. Cons. Stat. § 5725(a)) (citation modified). Vanguard advances two arguments in favor of dismissing the WESCA claim, neither of which persuades us.

First, Vanguard argues that plaintiffs have not alleged that the “contents” of their communications were disclosed to third parties, as is required for liability under WESCA. DI 13-1 at 22-23. WESCA defines the “contents” of a communication to “include[] any information concerning the substance, purpose, or meaning of [the] communication.” 18 Pa. Cons. Stat. § 5702. Because WESCA’s definition of “contents” is identical to the Federal Wiretap Act’s, decisions applying the Federal Act are instructive to understanding the scope of the term in WESCA. *Ingrao v. AddShoppers, Inc.*, No. CV 24-1022, 2024 WL 4892514, at *13 (E.D. Pa. Nov. 25, 2024). Under the Federal Wiretap Act, when the intercepted information shows “that the user is conducting a search for information on a particular topic,” that information amounts to the “substance” and “meaning” of a communication and thus reveals its “contents.” *Google Inc. Cookie Placement I*, 806 F.3d at 137-39 (quoting *[Redacted]*, No. PR/TT *[Redacted]* (FISA Ct. 2010), at 32). The same is true under WESCA. *See Ingrao*, 2024 WL 4892514, at *13 (noting that the disclosure of a search term can be the disclosure of the contents of a communication). Here, plaintiffs have plausibly alleged that the search terms they entered to look for financial

products — as well as their trading activity — were intercepted by LinkedIn, Google, and Meta. DI 12 ¶¶ 6-8, 87; *supra* IV.A. They thus plausibly allege that at least some “contents” of their communications were disclosed to those third parties.

Second, Vanguard argues that plaintiff Dy consented to any disclosure of his communications because they “knew or should have known about the disclosures in Vanguard’s [p]rivacy [n]otice, which was linked at the bottom of every page of Vanguard’s website” DI 13-1 at 24. But we cannot conclude that Dy consented based on the privacy notice at the motion to dismiss stage. Vanguard contends that even though this notice is not referenced in or attached to plaintiffs’ complaint, we may consider it as an “undisputedly authentic document” that plaintiffs’ claims are “based on.” DI 13-1 at 10 n.3 (quoting *Pension Benefit Guar. Corp. v. White Consol. Indus.*, 998 F.2d 1192, 1196 (3d Cir. 1993)). But the privacy notice serves as the basis for Vanguard’s defense, not plaintiffs’ claims. Moreover, even accepting for sake of argument that the privacy notice itself is an authentic document, Vanguard would still have to prove additional facts to show Dy’s consent. Vanguard would have to prove, at least, that the hyperlink was both functional and conspicuous enough for Dy to have reasonably seen it when they visited the website.³ We cannot make these extra-complaint factual findings on a motion to

³ See *James v. Glob. TelLink Corp.*, 852 F.3d 262, 267 (3d Cir. 2017) (“When terms are linked in obscure sections of a webpage that users are unlikely to see, courts have refused to find constructive notice.”); *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014) (“Where the link to a website’s terms of use is buried at the bottom of the page or tucked away in obscure corners of the website where users are unlikely to see it, courts have refused to enforce the browsewrap agreement.”); see also *Shah v. Cap. One Fin. Corp.*, 768 F. Supp. 3d 1033, 1044 (N.D. Cal. 2025) (“Because the issue of whether Plaintiffs consented to Defendant’s disclosure of their personal information is a factual question, the Court need not reach it at the motion to dismiss stage.”).

dismiss. *See T.D.H. v. Kazi Foods of New Jersey, Inc.*, No. CV 5:23-00634, 2023 WL 4567722, at *4 (E.D. Pa. July 17, 2023).

D. California Invasion of Privacy Act

The California Invasion of Privacy Act (CIPA) “broadly prohibits the interception of wire communications and disclosure of the contents of such intercepted communications.” *Ingrao*, 2024 WL 4892514, at *14 (quoting *Google Inc. Cookie Placement I*, 806 F.3d at 152).

Vanguard seeks dismissal of plaintiffs’ CIPA claims on both choice-of-law and merits grounds. We address each argument in turn.

1. Choice-of-law

At the threshold, Vanguard argues that the California plaintiffs’ CIPA claims must be dismissed because the parties agreed that Pennsylvania law, not California law, would govern this dispute. DI 13-1 at 25. Plaintiffs do not dispute that they agreed to the choice-of-law provision in Vanguard’s terms of use, which say that Pennsylvania law would apply in “any dispute that might arise between [plaintiffs] and Vanguard.” DI 12 ¶ 147. Rather, they argue that this choice-of-law provision does not control as to their CIPA claims. DI 19 at 22. We agree.

A federal court sitting in diversity applies the choice-of-law rules of the forum state. *SodexoMAGIC, LLC v. Drexel Univ.*, 24 F.4th 183, 204 (3d Cir. 2022). Here, we have jurisdiction over plaintiffs’ state law claims based on diversity as expanded by the Class Action Fairness Act. *See* DI 12 ¶ 10; *Levien v. hibu plc*, 475 F. Supp. 3d 429, 432 (E.D. Pa. 2020), *aff’d*, No. 20-2731, 2021 WL 5742664 (3d Cir. Dec. 2, 2021). We thus apply Pennsylvania choice-of-law rules in examining the enforceability of the choice-of-law provision.

“Pennsylvania courts will uphold an express choice of law provision if: ‘(1) the contract bears a reasonable relationship to the state whose law is chosen to govern’ and (2) ‘application of the chosen law does not violate a ‘strong public policy’ that would otherwise protect a party.’” *De Lage Landen Fin. Servs., Inc. v. Rasa Floors, LP*, 792 F. Supp. 2d 812, 825 (E.D. Pa. 2011) (quoting *Cottman Transmission Sys., Inc. v. Melody*, 869 F. Supp. 1180, 1183 (E.D. Pa. 1994)). Also relevant is whether one state “has a materially greater interest than the state of the chosen law in the determination of the particular issue.” *Kreider v. Green Robin Homes, LLC*, 2025 WL 1582461, at *14 (E.D. Pa. June 4, 2025) (quoting Restatement (Second) of Conflict of Laws § 187).

Here, California has strong policy interests in CIPA’s application to the alleged interception of the California plaintiffs’ communications, while Pennsylvania has essentially no interest in the application of WESCA to them. California “must be viewed as having a strong and continuing interest in the full and vigorous application of the provisions” of CIPA concerning the recording of telephone conversations, *Kearney v. Salomon Smith Barney, Inc.*, 137 P.3d 914, 935 (Cal. 2006), and this logic extends with equal force to provisions concerning the interception of online communications. Further, by arguing that WESCA requires the relevant communications to be intercepted in Pennsylvania, DI 13-1 at 23 n.6,⁴ Vanguard

⁴ Vanguard cites no authority in support of this territorial limitation, and it is not in WESCA’s text. But “Pennsylvania courts have declined to extend the WESCA to cover conduct occurring wholly outside the Commonwealth — at least in the context of recording telephone conversations.” *Popa*, 52 F.4th at 130 (citing *Larrison v. Larrison*, 750 A.2d 895, 898 (Pa. Super. Ct. 2000)). Because the parties have not raised the issue, we do not address whether their contractual choice-of-law provision might render WESCA applicable to conduct occurring outside of Pennsylvania. *Cf.* Carlos M. Vázquez, *Non-Extraterritoriality*, 137 Harv. L. Rev. 1290, 1291-96 (2024) (noting contractual choice-of-law clauses may permit courts to disregard statutes’ territorial scope limitations under some circumstances).

effectively concedes that applying Pennsylvania law would not protect this interest given that the California plaintiffs do not allege any interceptions of their communications in Pennsylvania.⁵ Moreover, accepting Vanguard’s concession that WESCA would not apply to communications intercepted outside Pennsylvania, Pennsylvania has little, if any, interest in ensuring that WESCA applies to conduct outside the state. We thus decline to enforce the parties’ choice-of-law agreement to apply WESCA to the California plaintiffs’ claims.

Having determined that the choice-of-law provision does not control, we conduct a traditional Pennsylvania choice-of-law analysis. *Holloway v. Fres-Co System USA, Inc.*, No. CV 13-3337, 2014 WL 796000, at *4 (E.D. Pa. Feb. 28, 2014). The first step in this analysis is to determine whether there is an “actual or real” conflict between California and Pennsylvania law — that is, whether the states’ laws are different. *Hammersmith v. TIG Ins. Co.*, 480 F.3d 220, 230 (3d Cir. 2007) (emphasis omitted). As discussed above, Vanguard does not dispute that WESCA requires that the relevant communications be intercepted in Pennsylvania, DI 13-1 at 23 n.6 — a requirement not present in CIPA. Hence, there is an actual or real difference between CIPA and WESCA, at least as applied here.

Having identified an actual or real conflict, our next step is to “examine the governmental policies underlying each law, and classify the conflict as a ‘true,’ ‘false,’ or an ‘unprovided-for’ situation.” *Hammersmith*, 480 F.3d at 230. A “true” conflict exists where both states’ policies would be impaired by the application of the other state’s law; a “false” conflict exists where only

⁵ Plaintiffs’ complaint does allege that California plaintiff “Felsen regularly logs into his account and searches for and purchases investments on the Website and App while in Pennsylvania,” but it is clear from context that plaintiffs meant to reference Pennsylvania plaintiff Dy here. DI 12 ¶ 8. Plaintiffs have confirmed that the reference to Felsen rather than Dy’s was a “scrivener’s error.” DI 19 at 20 n.4.

one state's policies would be so impaired; and an "unprovided-for" conflict exists where neither state's policies would be impaired. *Id.* at 230 & n.9; *Studer v. Avis Rent a Car System, LLC*, No. CV 23-3828, 2025 WL 950384, at *2 (E.D. Pa. Mar. 28, 2025). Here, there is a false conflict because only California's interests would be impaired by applying WESCA rather than CIPA to the California plaintiffs' claims. As discussed above, Pennsylvania has little if any interest in ensuring that WESCA applies to conduct in California that the statute does not regulate. Because there is a false conflict, we "must apply the law of the state whose interests would be harmed if its law were not applied," *Studer*, 2025 WL 950384, at *2 (citation omitted). Here, that is California's law.

2. Merits

CIPA, like WESCA, "broadly prohibits the interception of wire communications and disclosure of the contents of such intercepted communications." *Ingrao*, 2024 WL 4892514, at *14 (quoting *Google Inc. Cookie Placement I*, 806 F.3d at 152). Vanguard raises three arguments against liability under plaintiffs' CIPA theories, but all are derivative of arguments we have already rejected in evaluating plaintiffs' other claims. First, Vanguard argues that plaintiffs lack "statutory standing" under CIPA. DI 13-1 at 28-29. But to whatever extent the unpublished trial court order cited by Vanguard suggests an atextual, "statutory standing" injury requirement for CIPA, the court also suggested that it is co-extensive with Article III's. *Rodriguez v. Fountain9, Inc.*, No. CV 24-04504, 2024 WL 3886811, at *4 (Cal. Super. July 9, 2024) (citing *TransUnion*, 594 U.S. at 417). Vanguard's statutory standing argument thus fails for the same reasons as its Article III standing argument. *Supra* IV.A. Second, Vanguard argues that "CIPA's use of 'contents' has the same meaning as 'contents' under WESCA," and that the

CIPA claims thus fail for the same reasons as the WESCA claims. DI 13-1 at 29 (quoting *Ingrao*, 2024 WL 4892514, at *14). As discussed above, plaintiffs have plausibly alleged the interception of ‘contents’ under WESCA, and this argument as applied to CIPA fails for the same reasons. *Supra* IV.C. Third, Vanguard argues that plaintiffs fail to state a claim under CIPA because plaintiffs had no reasonable expectation of privacy in their communications. DI 13-1 at 29-30. We are unpersuaded at this stage, as explained above with respect to Vanguard’s Article III argument. *Supra* IV.A.⁶

E. California Invasion of Privacy

Vanguard argues that the California plaintiffs’ invasion of privacy claim under the California Constitution and state common law must be dismissed because Pennsylvania, not California law applies under the parties’ choice-of-law agreement. DI 13-1 at 30. Plaintiffs do not respond to this argument — they provide no argument as to why California law applies to this claim notwithstanding the choice-of-law provision, nor do they argue that it could be brought under Pennsylvania law. *See* DI 19 at 25-26. Therefore, plaintiffs have forfeited their invasion of privacy claims. *Bonsall v. County of Delaware*, No. CV 24-5866, 2026 WL 499908, at *12 (E.D. Pa. Feb. 23, 2026) (“[A] party’s failure to respond to an argument ‘acts as a concession of that argument.’” (quoting *Sang Geoul Lee v. Won Il Park*, 720 F. App’x 663, 666 (3d Cir. 2017))). Accordingly, we agree that these claims should be dismissed.

⁶ Vanguard also suggests that it is not liable under Clause One of CIPA § 631(a) and that plaintiffs have no claim for equitable relief. DI 13-1 at 29, DI 20 at 13. Plaintiffs have conceded that they are not seeking to impose liability under Clause One of CIPA § 631(a) and that they are not entitled to equitable relief. DI 19 at 25 & n.1. Thus, we do not address Vanguard’s arguments with respect to these theories, with the understanding that plaintiffs may not seek to revive these theories. *See Petroski v. First Horizon Home Loans Inc.*, No. CV 02-8022, 2004 WL 1551736, at *2 (E.D. Pa. July 9, 2004).

V. Conclusion

For the reasons discussed above, we dismiss plaintiffs' Federal Wiretap Act claims and their California Invasion of Privacy claims. Because plaintiffs have already amended their complaint and because plaintiffs' briefing fails to advance legal arguments in support of these theories, we could dismiss these claims with prejudice. But in an abundance of caution, we will dismiss without prejudice. We deny Vanguard's motion to dismiss plaintiffs' remaining claims.