UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

FRANK D. RUSSO, ET AL.,

Plaintiffs,

vs.

MICROSOFT CORPORATION,

Defendant.

CASE NO. 4:20-cv-04818-YGR

ORDER GRANTING DEFENDANT MICROSOFT CORPORATION'S MOTION TO DISMISS PLAINTIFF'S COMPLAINT

Re: Dkt. No. 25

Plaintiffs Frank D. Russo; Koonan Litigation Consulting, LLC; and Sumner M. Davenport & Associates, LLC (collectively, "Plaintiffs") bring this class action against Defendant Microsoft Corporation for violation of privacy laws. (Dkt. No. 29 ("Comp.").) Plaintiffs allege violations of (1) the Wiretap Act, 18 U.S.C. § 2511, *et seq.*, (2) the Stored Communications Act ("SCA"), 18 U.S. C. § 2701 *et seq.*, (3) the Washington Consumer Protection Act ("WCPA"), Wash. Rev. Code 9,73.010 *et seq.*, (4) Washington Privacy Act ("WPA"), Wash. Rev. Code 9.73.010 *et seq.*, and (5) intrusion upon seclusion under Washington law.

Now before the Court is Microsoft's motion to dismiss. (Dkt. No. 25 ("Mot.").) Having considered the papers submitted and the pleadings in this action, and for the reasons below, the Court hereby **GRANTS IN PART** and **DENIES IN PART** the motion to dismiss.[1]

I. BACKGROUND

Plaintiffs use Microsoft's software to conduct business. Mr. Russo uses Microsoft 365 Business Standard for his sole proprietorship, Russo Meditation & Law, to provide mediation, arbitration, and alternative dispute resolution services to clients. (Comp. ¶¶ 13-15.) Koonan Litigation Consulting, LLC employs Microsoft 356 Business Basic to provide advice on "all

[1] The Court finds the motion appropriate for resolution without oral argument and the

aspects of litigation." (*Id.* ¶¶ 20-23.) Sumner M. Davenport & Associates, LLC similarly uses Microsoft 365 Business Basic to provide marketing services. (*Id.* ¶¶ 28-34.) Each product provides cloud-based access to Microsoft's Office software suite for a monthly subscription fee. (*Id.* ¶ 46.)

Plaintiffs allege that Microsoft (1) shared its business customers' data with Facebook, (2) shared its business customers data with third-party developers, (3) shared its business customers' data with subcontractors to support Microsoft's products, and (4) used business customers' data to develop and sell new products and services through their software without consent. (*Id.* ¶ 1.)

Although the precise nature of plaintiffs' claims lacks clarity, the complaint appears to quote from various documents related to different features.[2] First, with respect to Facebook data sharing, plaintiffs quote from a technical document describing "Facebook Contact Sync," which "shares information in your Outlook Contacts folder with Facebook and imports your Facebook friends' contact information into your Outlook Contacts folder." (*Id.* ¶ 76; Dkt. No. 25-1 at 12.) Although the complaint acknowledges that this feature can be disabled, it states that "the damage has already been done" at that point because "[o]nce contacts are transferred to Facebook, they cannot be deleted from Facebook's system except by Facebook." (Comp. ¶ 76.)

Second, with respect to third-party developers, plaintiffs apparently refer to "Microsoft Graph," which allows developers to "build smarter apps" for Windows using APIs that "model and represent people in Microsoft 365 services," including by "perform[ing] searches for people who are relevant to the signed-in user and have expressed an interest in communicating with that user over certain 'topics.'" (*Id.* ¶ 84; Dkt. No. 25-1 at 51, 53.) Although plaintiffs apparently acknowledge that this feature requires user permission, they allege that "Microsoft nonetheless transmits [a] non-consenting business customer's data to third-party developers if *another* Office 365 user consented to the application." (Comp. ¶ 82 (emphasis in original); *see* Dkt. No. 25-1 at

[2] The Court **GRANTS** Microsoft's request for judicial notice of these documents. (Dkt. No. 25-2.) The statements in these documents form the basis of Plaintiffs' claims and are therefore incorporated by reference. *See Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1022 (9th Cir 2018). Plaintiffs do not oppose Microsoft's request, but, on the contrary, also quote from those

53.) For instance, if a signed-in user give consent, the API allows a developer to search that user's email to find other users who have communicated about particular topics. (*See id.*)

Third, with respect to subcontractors, plaintiffs allege generally that Microsoft uses subcontractors "not only to provide customers with the services they purchased, but also to serve Microsoft's separate commercial ventures, including discovering new business insights and developing new services, products, or features," without requiring anonymization or encryption. (Comp. ¶¶ 87-90.) The factual basis for this claim is not alleged.

Finally, with respect to using data to develop new products, plaintiffs refer to the following products: Security Graph API, Microsoft Audience Network, Windows Defender Application Control, Azure Advanced Threat Protection, Advanced Threat Protection, and Cortana. (*Id.* ¶¶ 93-97.) Plaintiffs allege facts for only the first two products and Cortana. Security Graph is an API provided to developers "so they can create new security-related products" that is allegedly built by "scanning '400 billion' . . . customers' emails and 'data from 700 million Azure user accounts.'" (*Id.* ¶¶ 93-94.) Microsoft Audience Network appears to be an advertisement product that imparts "rich user understanding" through "robust data sets." (*Id.* ¶ 95.) Cortana allegedly "collects and uses business customer data (including documents, contacts, and calendar information)" to "develop and improve" its service. (*Id.* ¶ 97.)

Plaintiffs claim that Microsoft's practices are contrary to its marketing representations and contracts, which tout its privacy protections. (*Id.* § B.) For instance, Microsoft's "Trust Center" website allegedly states that "[w]e use your data for just what you pay us for: to maintain and provide Office 365" and "only to provide the services." (*Id.* ¶ 58.) Its Online Service Terms similarly allegedly state that it will use customer data only to "[d]eliver[] functional capabilities," "troubleshoot[] problems," and "improv[e] the product through updates." (*Id.* ¶ 65.) Indeed, the terms allegedly promise that customer data will not be used for "(a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions." (*Id.* ¶ 66.) Plaintiffs claim that they would not have purchased Microsoft's products if they knew the truth about their use. (*Id.* ¶ 114.)

II. LEGAL STANDARD

Under Federal Rule of Civil Procedure 12(b)(6), a complaint may be dismissed for failure to state a claim upon which relief may be granted. Dismissal for failure under Rule 12(b)(6) is proper if there is a "lack of a cognizable legal theory or the absence of sufficient facts alleged under a cognizable legal theory." *Conservation Force v. Salazar*, 646 F.3d 1240, 1242 (9th Cir. 2011) (quoting *Balistreri v. Pacifica Police Dep't*, 901 F.2d 696, 699 (9th Cir. 1988)). The complaint must plead "enough facts to state a claim [for] relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim is plausible on its face "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678. If the facts alleged do not support a reasonable inference of liability, stronger than a mere possibility, the claim must be dismissed. *Id*. at 678-79; *see also In re Gilead Scis. Sec. Litig.*, 536 F.3d 1049, 1055 (9th Cir. 2008) (stating that a court is not required to accept as true "allegations that are merely conclusory, unwarranted deductions of fact, or unreasonable inferences").

If a court dismisses a complaint, it should give leave to amend unless "the pleading could not possibly be cured by the allegation of other facts." *Cook, Perkiss & Liehe, Inc. v. N. Cal. Collection Serv. Inc.*, 911 F.2d 242, 247 (9th Cir. 1990).

III. ANALYSIS

A. Plaintiffs Have Not Shown Standing.

To bring a claim in federal court, a plaintiff needs to have standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 559-60 (1992). Article III standing requires plaintiffs to have "(1) suffered injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, -- U.S. --, 136 S. Ct. 1540, 1547 (2016). Plaintiffs who have not been personally injured in by defendant's conduct lack a "personal stake" in the outcome and thus have no standing. *Id*. at 1548; *see also Raines v. Byrd*, 521 U.S. 811, 818-19 (1997). The party invoking federal jurisdiction must "clearly allege facts demonstrating each element" of standing at the motion to dismiss stage. *Spokeo*, 136 S.Ct at 1547 (simplified).

Here, plaintiffs do not allege enough facts to draw a reasonable inference that they have been injured by Microsoft's conduct. With respect to Facebook Connect, plaintiffs do not allege that they have used Outlook, much less that they added anyone to their Outlook Contacts folder who could have been disclosed to Facebook. With respect to third-party developers, plaintiffs do not allege any user with whom they communicated that granted consent for Microsoft Graph to scan their emails. With respect to both subcontractors and Microsoft's other products, plaintiffs do not allege any facts that could support a reasonable inference that Microsoft's cloud software customers were affected at all. For instance, plaintiffs do not explain how the information for Advanced Threat Protection was gathered and how involved Office 365 customers.

Instead, plaintiffs cite two paragraphs that generically state that Microsoft used and shared "Plaintiffs' and Class Members'" data, including their emails, as described above. (*See* Comp. ¶¶ 141, 143.) Such allegations are far too sparse and conclusory to make the claim of personal injury plausible. *See Gilead*, 536 F.3d at 1055; *cf. In re Chrysler-Dodge-Jeep Ecodiesel Mktg., Sales Practices, & Product Liability Litig.*, 295 F. Supp. 3d 927, 949 (N.D. Cal. 2018) (no standing based on overpayment theory where plaintiffs do not allege that *their* products were defective). The Court thus dismisses the complaint for failure to allege facts demonstrating standing.[3]

B. Plaintiffs Have Not Stated a Claim.

For similar and additional reasons, plaintiffs have failed to state a claim on the merits. As an initial matter, plaintiffs' allegations concerning subcontractors and use of customer data to develop new products (the third and fourth set of alleged conduct) are too conclusory to render their claims plausible. Based on plaintiffs' complaint, Microsoft *could* be using customer data and

[3] In addition to Article III, the statutes here limit the types of injuries sufficient for a party to bring suit. The Wiretap Act provides a cause of action only to persons "whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used." 18 U.S.C. § 2520. The SCA provides a cause of action to a person "aggrieved by any violation," 18 U.S.C. § 2707(a), which typically requires a plaintiff to "allege[] with particularity that *her* communications were part of the [disclosure]." *Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 910 (9th Cir. 2011) (emphasis in original). Further, the WPA provides a cause of action only to those "claiming that a violation of this statute has injured his or her business, his or her person, or his or her reputation." Wash. Rev. Code § 9.73.060. Thus, because plaintiffs fail to allege Article III standing, they also fail to state a claim under these statutes.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.