2021 WL 2983198
Only the Westlaw citation is currently available.
United States District Court, E.D. California.

DEREK MASTEL, individually and on behalf of all others similarly situated, Plaintiff,
v.
MINICLIP SA; APPLE INC., Defendants.

No. 2:21-cv-00124 WBS KJN
|
07/15/2021

ORDER RE: DEFENDANTS' MOTIONS TO DISMISS

***1** Plaintiff Derek Mastel brought this putative class action against defendants Miniclip SA ("Miniclip") and Apple Inc. ("Apple"), claiming that they violated the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631, and California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, and invaded his privacy under the California Constitution via an app developed by Miniclip for use on Mastel's iPhone. (See generally Compl. (Docket No. 1).) Mastel's complaint also brings a claim under the Federal Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, solely against Miniclip. (Compl. ¶ 62.) Defendants now move to dismiss plaintiff's claims in their entirety. (See Apple's Mot. to Dismiss (Docket No. 8); Miniclip's Mot. to Dismiss (Docket No. 21).)

I. Factual Background

Miniclip is a developer of videogames that can be played on web browsers or downloaded as mobile applications and played on various electronic devices, including iPhones. (Compl. ¶¶ 5, 14.) This case centers around one of Miniclip's iPhone games known as 8 Ball Pool. (See Compl. ¶¶ 1-3.)

Apple manufactures and sells iPhones. (Compl. ¶ 10.) All iPhones run on an operating system known as iOS. (Id.) One feature of iOS that is relevant to this case is the "Pasteboard," which is similar to the copy-paste function on a computer. (Compl. ¶ 11.) Pasteboard allows the user to copy text while using one application and paste it into another application. (Id.) For instance, as noted in the complaint, a user might "copy an Internet address from a web browser to the Pasteboard and paste the Internet address in a text message." (Id.)

The Pasteboard itself only saves one set of copied text at a time; as soon as a user copies another set of text, any previously saved text is deleted. (Compl. ¶ 12.) However, Apple authorizes mobile applications to view, copy, and save the text stored in the Pasteboard any time the user opens the application. (Compl. ¶¶ 12, 17) Thus, a mobile application developer may program its application to save and compile a library of text that iPhone users have copied into the Pasteboard while the application is open. (Compl. ¶¶ 12, 17-18.)

Mastel downloaded 8 Ball Pool onto his iPhone in 2013. (Compl. ¶ 22.) Mastel alleges that 8 Ball Pool accessed the Pasteboard on his iPhone each time he opened the application, without his knowledge or consent. (Compl. ¶¶ 24, 29.) Mastel's complaint provides a screenshot of 8 Ball Pool's "device log," which provides a list of the functions performed by the application with corresponding timestamps in chronological order. (Compl. ¶ 19.) The device log purportedly shows 8 Ball Pool requesting access to and reading the contents of the Pasteboard. (See id.)

Mastel does not specifically allege how many times he opened 8 Ball Pool over the eight-year period it has been on his iPhone, or what information was on the Pasteboard each time he opened it. (See id.) Rather, he alleges that, since he downloaded 8 Ball Pool in 2013, he "has copied numerous sets of text" into the Pasteboard, including his name, email, phone number, and address, addresses of friends and relatives, and personal and private messages that have been sent to friends and relatives. (Compl. ¶ 23.) Mastel alleges that Miniclip had access to all of the data stored in the 8 Ball Pool application. (Compl. ¶¶ 26-27.)

II. Discussion

***2** Federal Rule of Civil Procedure 12(b)(6) allows for dismissal when the plaintiff's complaint fails to state a claim upon which relief can be granted. See Fed. R. Civ. P. 12(b)(6). The inquiry before the court is whether, accepting the allegations in the complaint as true and drawing all reasonable inferences in the plaintiff's favor, the complaint has stated "a claim to relief that is plausible on its face." Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007). "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009).

"Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." Id. Although legal conclusions "can provide the framework of a complaint, they must be supported by factual allegations." Id. at 679.

A. California Invasion of Privacy Act

Mastel's first claim is that defendants violated § 631(a) of the CIPA, which addresses "wiretapping." (See Compl. ¶¶ 39-51); Cal. Penal Code § 631(a). Section 631(a) imposes liability upon

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained....

Id.

The California Supreme Court has explained that this lengthy provision contains three operative clauses covering "three distinct and mutually independent patterns of conduct": (1) "intentional wiretapping," (2) "willfully attempting to learn the contents or meaning of a communication in transit over a wire," and (3) "attempting to use or communicate information obtained as a result of engaging in either of the two previous activities." Tavernetti v. Superior Court, 22 Cal. 3d 187, 192 (Cal. 1978); accord In re Google Inc., No. 13-MD-02430-LHK, 2013 WL 5423918, at *15 (N.D. Cal. Sept. 26, 2013). Section 631(a) further contains a fourth basis for liability, for anyone "who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the" other three bases for liability. Cal. Penal Code § 631(a).

As an initial matter, Mastel concedes in his opposition that he has only brought his § 631(a) claim against Apple under the fourth clause. (Pl.'s Opp'n at 3.) Thus, while Mastel argues that Miniclip may be found liable under any of § 631(a)'s four clauses, Apple may only be liable if the court finds that it "aid[ed], agree[d] with," or "conspire[d]" with Miniclip to violate § 631(a).

1. Intentional Wiretapping

Beginning with § 631(a)s' first clause, in order to plausibly state a claim, Mastel must allege that Miniclip "intentionally tap[ped], or ma[de] any unauthorized connection . ..with any telegraph or telephone wire, line, cable, or instrument...." Cal. Penal Code § 631(a). Miniclip argues that Mastel's allegations are insufficient because, at most, they show that the 8 Ball Pool App tapped or made an unauthorized connection with the iOS Pasteboard, which is not a "telegraph or telephone wire, line, cable, or instrument." (Miniclip Mot. to Dismiss at 4-5; FAC ¶¶ 22-25.)

***3** Mastel cites to several decisions by federal courts interpreting the CIPA for the proposition that the statute should be read broadly to encompass new technologies that have developed since its enactment. See Matera v. Google Inc., No. 15-CV-04062-LHK, 2016 WL 8200619, *19 (N.D. Cal. Aug. 12, 2016) ("[T]he California Supreme Court has construed CIPA in accordance with the interpretation that provides the greatest privacy protection."); In re Google Inc., No. 13-MD-02430-LHK, 2013 WL 5423918, *21 (N.D. Cal. Sep. 26, 2013) (noting that the California Supreme Court "regularly reads statutes to apply to new technologies where such a reading would not conflict with the statutory scheme"); Revitch v. New Moosejaw, LLC, No. 18-cv-06827-VC, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019).

While it is true that several federal courts interpreting the CIPA have held that the statute may apply to technologies beyond telephones or telegraphs, those holdings have largely been limited to the statute's second clause, which prohibits persons from reading, or attempting to read, the "contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable" without consent or authorization. See Matera, 2016 WL 8200619, at *18 (finding that § 631(a)'s first prong is "limited to communications passing over 'telegraph or telephone' wires, lines, or cables"); In re Google Inc., 2013 WL 5423918, at *20 (explaining that the first prong of CIPA is "limited to communications passing over 'telegraphic or telephone' wires, lines, or cables"); accord In re Google Assistant Priv. Litig., 457 F. Supp. 3d 797, 979, 826 (N.D. Cal. 2020) ("Google Assistant") (holding that CIPA claim under first clause must be dismissed if allegations do not show that technology at issue "operates using telegraph or telephone wires").

At oral argument, counsel for Mastel cited New Moosejaw for the proposition that § 631(a)'s first prong may apply to technologies beyond telephones or telegraphs. See New Moosejaw, LLC, 2019 WL 5485330, at **1-2. In New Moosejaw, however, the court simply assumed that § 631(a) could apply to customer interactions with a website, and instead focused its analysis on whether such interactions constitute a "communication" under the statute. See id. Though the court did not specify which clause of § 631(a) it was analyzing, the word "communication" only appears in § 631(a)'s second clause. See Cal. Penal Code § 631(a). It is therefore unlikely that New Moosejaw intended to implicitly hold that § 631(a)'s first clause may apply to new technologies like the internet. See id. Moreover, in a supplemental response filed two days after the hearing, counsel for Mastel conceded that New Moosejaw does not support his argument that Miniclip may be held liable under § 631(a)'s first clause. (See Docket No. 37.) The court will therefore follow the overwhelming weight of authority requiring a plaintiff to plausibly allege that a defendant intentionally tapped or made an unauthorized connection with a "telegraph or telephone wire, line, cable, or instrument" to state a claim under § 631(a)'s first clause. Cal. Penal Code § 631(a) (emphasis added).

Mastel's complaint plainly does not involve any allegations concerning "telephone wires, lines, or cables." (See generally Compl.) Mastel contends, however, that the Pasteboard falls within the text of the statutory prohibition because it may be considered a "telephone instrument." (See Pl.'s Opp'n at 4.) Mastel cites dictionary.cambridge.org for the following definition of "instrument": "a tool or other device used for doing a particular piece of work." (Id. (citing INSTRUMENT, https://dictionary.cambridge.org/us/dictionary/English/instrument ).) Because the Pasteboard is a "tool or device" exclusive to iPhones, Mastel contends, it qualifies as a "telephone instrument." (See FAC ¶¶ 10-11.)

***4** The court rejects this argument. Although iPhones contain the word "phone" in their name, and have the capability of performing telephonic functions, they are, in reality, small computers. iPhones contain a complex operating system which allows the user to download mobile applications that perform functions well beyond and unrelated to those of a telephone. (See Compl. ¶¶ 10-15.) The Pasteboard, which permits iPhone users to copy and paste text from one application to another, is a feature of the portion of the iPhone that functions as a computer, not the phone. (Compl. ¶ 11.) While Pasteboard may enable an iPhone user to paste a phone number into the phone application, labeling it a "telephone instrument" for this reason would be analogous to calling a pen and paper "telephone instruments" because they allow a caller to write down a phone number before dialing. The court therefore finds that § 631(a)'s first clause does not apply to Miniclip's conduct as alleged in the complaint. See Cal. Penal Code § 631(a).

2. Willfully Attempting to Learn the Contents of Communications in Transit Over a Wire

Under § 631(a)'s second clause, Mastel must allege that Miniclip "willfully and without the consent of all parties to the communication, or in any unauthorized manner, read[ ], or attempt[ed] to read, or to learn the contents or meaning of any message, report, or communication while the same [was] in transit or passing over any wire, line, or cable, or [was] being sent from, or received at any place within [California]." Id.

As discussed above, unlike § 631(a)'s first clause, courts interpreting the second clause have generally held that it is not limited to communications sent via telephone or telegram wire, line, or cable. See Matera, 2016 WL 8200619, at *18; In re Google Inc., 2013 WL 5423918, at *20; Google Assistant, 457 F. Supp. 3d at 826. However, these courts have also noted that the second clause only imputes liability when the defendant reads, or attempts to read, a communication that is "in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within" California." Id. (emphasis added); see also Mireskandari v. Mail, No.

CV 12-02943 MMM (FFMx), 2013 WL 12129559, *10 n.44 (C.D. Cal. July 30, 2013) (finding that plaintiff had failed to plausibly allege CIPA claim under second clause because complaint failed "plausibly to plead that NSC intercepted any electronic communication while it was in transit; at most, he alleges the illegal disclosure of data NSC held in storage").

Here, Mastel's complaint does not contain any allegations that Miniclip intercepted any communications while they were "in transit," as they were "passing over" a line, wire, or cable, or as they were "being sent" or "received." Cal. Penal Code § 631(a). As the complaint alleges, text ends up in the Pasteboard because the user copies it from another application. (See Compl. ¶¶ 10-29.) The complaint does not allege that the Pasteboard is in any way involved in or necessary to the iPhone's mechanism for sending or receiving communications such as text messages or emails. (See id.) Thus, to the extent that Mastel's complaint alleges that the 8 Ball Pool application obtained the content of his communications, this content could only have come from previously-sent or previously-received communications that Mastel chose to copy into the Pasteboard. There are simply no allegations in the complaint that reasonably give rise to the inference that the 8 Ball Pool App ever read or learned the contents of a communication while the communication was in transit, or in the process of being sent or received. See Iqbal, 556 U.S. at 678.

Mastel next argues that the CIPA's second clause may be satisfied because he has adequately alleged that the Pasteboard performs a "transitory electronic storage" function. Citing two cases interpreting the analogous Federal Wiretap Act, In re Carrier IQ, Inc., 78 F. Supp. 3d 1057, 1081 (N.D. Cal. 2015) ("Carrier IQ") and United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005), Mastel contends that some courts have concluded that a defendant "intercepts" a communication when he acquires it from "transitory electronic storage" that is part of the overall message transmission process.

***5** While some cases have looked to the Federal Wiretap Act for guidance in evaluating claims under the CIPA, see, e.g., In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589, 606-07 (9th Cir. 2020) ("Facebook Tracking"), the court does not find Mastel's reliance on those cases to be persuasive in the context of this case. As Carrier IQ itself notes, the Ninth Circuit has expressly held that, for an electronic communication to be "intercepted," it must have been "acquired during transmission, not while it is in electronic storage." Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002). Thus, even to the extent the Pasteboard does perform transitory storage functions, the Ninth Circuit's interpretation of the Federal Wiretap Act only reinforces the court's conclusion that the crucial question under § 631(a)'s second clause is whether Mastel has plausibly alleged that Miniclip read one of his communications while it was still in transit, i.e., before it reached its intended recipient. See Mireskandari, 2013 WL 12129559, at *10 n.44. Because the complaint fails to do so, the court finds that his complaint fails to state a claim against Miniclip under § 631(a)'s second clause.

Because the court concludes that Mastel has failed to state a claim under either clause 1 or 2, his claim that Miniclip violated § 631(a)'s third clause fails as a matter of law. See Google Assistant, 457 F. Supp. 3d at 827 ("Plaintiffs must establish that the information at issue...was obtained through a violation of the first or second clauses. Because plaintiffs have not done so, they also have failed to plead a violation of the third clause."). Likewise, because Mastel has failed to establish an underlying violation, Mastel cannot maintain a claim against Apple under the fourth clause because none of the alleged conduct that Apple allegedly "agreed to" or "aided" violated § 631(a). See Cal. Penal Code § 631(a).

Accordingly, the court will dismiss plaintiff's first claim against defendants for violations of the CIPA § 631(a).

B. Right to Privacy under the California Constitution

Mastel next claims that defendants' behavior violated his right to privacy under the California Constitution. To state a claim under the California constitutional right to privacy, a plaintiff "must show that (1) [he] possess[es] a legally protected privacy interest, (2) [he] maintain[s] a reasonable expectation of privacy, and (3) the intrusion is 'so serious... as to constitute an egregious breach of the social norms' such that the breach is 'highly offensive.' " In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589, 601 (9th Cir. 2020) ("Facebook Tracking") (quoting Hernandez v. Hillsides, Inc., 47 Cal. 4th 272, 286 (Cal. 2009)).

1. Standing

Miniclip first argues that Mastel lacks standing to pursue his claim for violation of his right to privacy under the California Constitution. (Miniclip Mot. to Dismiss at 10.)

  

"Where standing is raised in connection with a motion to dismiss, the court is to 'accept as true all material allegations of the complaint, and...construe the complaint in favor of the complaining party.' " Facebook Tracking, 956 F.3d at 601 (quoting Levine v. Vilsack, 587 F.3d 986, 991 (9th Cir. 2009)).

To establish standing, a "[p]laintiff must have (1) suffered an 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 v. Robins, 578 U.S. 330, 336 (2016). To establish an injury in fact, a plaintiff must show that he or she suffered "an invasion of a legally protected interest" that is "concrete and particularized." Id. at 337 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)). A concrete injury is one that is "real and not abstract." Id.

In a recent decision, TransUnion LLC v. Ramirez, 594 U.S. --, -- S. Ct. --, 2021 WL 2599472 (Jun. 25, 2021), the Supreme Court provided additional guidance to lower courts tasked with assessing whether a plaintiff's alleged harm is adequately "concrete" so as to confer Article III standing. See TransUnion, 2021 WL 2599472, at *7. The Court explained that, while certain harms, such as physical and monetary harms, "readily qualify as concrete injuries under Article III," other intangible injuries, such as "reputational harms, disclosure of private information, and intrusion into seclusion," may nevertheless qualify as "concrete" as well, even though they are harder to discern. Id. (citing Spokeo, 578 U.S. at 340-41).

***6** The Court noted that the chief examples of such intangible injuries that are nevertheless "concrete" are those "with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts." Id. It also explained that, though the view of Congress may be instructive in the sense that it may "elevate to the status of legally cognizable injuries concrete, de facto injuries that were previously inadequate in law," Congress may not "simply enact an injury into existence, using its lawmaking power to transform something that is not necessarily harmful into something that is." Id. (citing Spokeo, 578 U.S. at 341).

Applying these principles to the case before it, the Court held that certain members of the putative class had failed to allege that TransUnion had caused them a "concrete" injury when it failed to use reasonable procedures to ensure the accuracy of their credit files. Id. at *14. Though Congress had enacted a statute authorizing the plaintiffs to sue when a credit reporting agency negligently created inaccurate credit files, and TransUnion had concededly violated the terms of that statute, the Court held that the plaintiffs had not alleged a concrete injury because TransUnion had not disseminated the inaccurate credit files to any third parties. See id. at **11-14.

Miniclip argues that Mastel has similarly failed to adequately allege an injury in fact because he offers only a "conclusory assertion of a privacy violation." (Miniclip Mot. to Dismiss at 10.) Miniclip contends that, without some allegation that it shared or otherwise published Mastel's private information, such that it became known to a third party, Mastel has not adequately alleged a "concrete" harm that resulted from Miniclip's alleged invasion of his privacy. (Miniclip Reply at 6-7 (Docket No. 30) (citing TransUnion, 2021 WL 2599472, at *3.)

The court finds TransUnion to be distinguishable from this case, however, because TransUnion involved a fundamentally different type of alleged injury than the one here. TransUnion concerned a violation of a statute which the Supreme Court analogized to the common law tort of defamation. See TransUnion, 2021 WL 2599472, at *10. The Court held that the plaintiffs had not alleged a "concrete" harm because "publication is 'essential to liability' in a suit for defamation." Id. at *11 (quoting Restatement of Torts § 577, Comment a, at 192).

By contrast, the closest historical analogue to plaintiff's invasion of privacy claim under the California Constitution is not defamation, but other "invasion of privacy" torts such as intrusion upon seclusion. Facebook Tracking, 956 F.3d at 598 ("[V]iolations of the right to privacy have long been actionable at common law."). The Ninth Circuit has expressly noted that, because the right to privacy "encompasses the individual's control of information concerning his or her person," allegations that a company has violated a plaintiff's right to privacy under the California Constitution by collecting personal information without the plaintiff's consent involve a sufficiently "concrete" injury, even if there are no additional allegations of publication, because the invasion itself causes harm to the plaintiff's interest in controlling the information. Id.; see also Eichenberger v. ESPN, Inc., 876 F.3d 979, 983 (9th Cir. 2017) (""privacy torts do not always require additional consequences to be actionable...[in] the tort of intrusion upon seclusion...the 'intrusion itself' makes the defendant liable" (citing Restatement (Second) of Torts § 652B cmt. b. (Am. Law Inst. 1977))).

  

Though Facebook Tracking and Eichenberger were decided before TransUnion, they are not overruled by TransUnion. TransUnion involved a claim akin to defamation, not invasion of privacy. The court therefore finds Facebook Tracking and Eichenberger to be more on point, and rejects Miniclip' argument that plaintiff must necessarily allege that it shared or otherwise disseminated his private information in order to satisfy Article III's standing requirement.

2. Egregious Breach of Social Norms

***7** Next, both Apple and Miniclip argue that, even if Mastel has standing to pursue an invasion of privacy claim against them under the California Constitution, any alleged intrusion by Miniclip into the iPhone's Pasteboard fails to satisfy the third element of an invasion of privacy claim because it does not rise to the level of an "egregious breach of social norms" that is "highly offensive." Facebook Tracking, 956 F.3d at 601.

As an initial matter, the court recognizes that questions of whether conduct is "egregious," "offensive," or violates "social norms" tend by their very nature to be subjective determinations about which reasonable jurists may differ. As such, these questions are typically more appropriately resolved by a jury. Social norms, as reflections of contemporary community values, necessarily change over time. What was "egregious" or "offensive" at one time and place may be completely unobjectionable, or even laudable, in another.

"That the jury provides a better link to community values than does a single judge is supported not only by our cases, but also by common sense." Spaziano v. Florida, 468 U.S. 447, 486 (1984) (Stevens, J., concurring). "Juries--comprised as they are of a fair cross section of the community--are more representative institutions of the community as a whole, and inevitably make decisions based on community values more reliably, than can that segment of the community that is selected for service on the bench." Id. Indeed, as Justice Gorsuch recently observed, judges are "hardly the representative group you'd expect (or want) to be making empirical judgments" as to what values society at large holds. Carpenter v. United States, 138 S. Ct. 2206, 2265 (2018) (Gorsuch, J., dissenting). "Politically insulated judges come armed with only the attorneys' briefs, a few law clerks, and their own idiosyncratic experiences ...[u]nsurprisingly, too, judicial judgments often fail to reflect public views." Id.

For those reasons, if the court were left to rely only upon its own subjective opinion, without any objective criteria from the statutes or caselaw defining what constitutes "egregious," or "highly offensive" conduct in breach of "social norms", it would be hesitant to make such determination at the motion to dismiss stage. See In re Facebook, Inc., Consumer Privacy User Profile Litigation, No. 18-MD-02843-VC, 2019 WL 4261048, at *17.

However, in the context of claims under the California Constitution for invasion of privacy, the California courts have provided some clear and objective guidance as to the trial courts' role in applying those terms at the pleading stage. In Loder v. City of Glendale, 14 Cal. 4th 846, 893 (Cal. 1997), the California Supreme Court instructed that courts have a role to play in "weed[ing] out claims that involve so insignificant or de minimus an intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant." "No community could function if every intrusion into the realm of private action, no matter how slight or trivial, gave rise to a cause of action for invasion of privacy." Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1, 37 (Cal. 1994). Accordingly, if the "undisputed material facts show...an insubstantial impact on privacy interests, the question of invasion may be adjudicated as a matter of law." Id. at 40.

Miniclip cites to no less than twelve cases in which courts have dismissed an invasion of privacy claim under the California Constitution at the pleading stage. (See Miniclip Mot. to Dismiss at 10-12.) While no hard-and-fast rule has been set out for determining when an alleged invasion of privacy is "sufficiently serious in [its] nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right," Hill, 7 Cal. 4th at 37, one important factor that courts often rely on is whether the plaintiff alleges that the defendant used the private or confidential information obtained for some improper purpose.

***8** In Gonzales v. Uber Technologies, Inc., for instance, the court held that the plaintiff had failed to state a claim under the California Constitution against Uber because, while he had alleged that Uber obtained his name and home address, "there [were] no allegation[s] as to what Uber did, if anything, with this information." 305 F. Supp. 3d 1078, 1092 (N.D. Cal. 2018). "Without more allegations as to what, if anything, Uber did with this information, plaintiff has not plausibly alleged a serious invasion of privacy." Id. at 1093.

Similarly, in White v. Social Security Administration, applying California law, a federal district court held that plaintiff's invasion of privacy claim failed because, while the plaintiff had alleged that the defendant had "made unauthorized photocopies of identity documents, without any allegation that he sold, distributed, or otherwise improperly used the information," the plaintiff had failed to adequately allege a sufficiently serious invasion of privacy. 111 F. Supp. 3d 1041, 1053 (N.D. Cal. 2015). Even in Folgelstrom v. Lamps Plus, Inc., where the plaintiff had alleged that the defendant had obtained his name and zip code through misrepresentation and then used this information to obtain his address so that it could send him mailed advertisements, the court dismissed the plaintiff's claim because the alleged use was "not an egregious breach of social norms, but routine commercial behavior." 195 Cal. App. 4th 986, 992 (2d Dist. 2011) ("[W]e have found no case which imposes liability based on the defendant obtaining unwanted access to the plaintiff's private information which did not also allege that the use of plaintiff's information was highly offensive.").

In this case, Mastel has not alleged that Miniclip or Apple used his information for any purpose at all, much less a purpose that could plausibly constitute an egregious breach of social norms. Though Mastel alleges that Miniclip has access to all of the data collected in the 8 Ball Pool application, including the information collected from his Pasteboard, he does not allege that Miniclip "sold, distributed, or otherwise improperly used the information." See White, 111 F. Supp. 3d at 1053. Nor has he even alleged that defendants intended to use his information for any purpose. Mastel's counsel also admitted at oral argument that the complaint does not even allege that Miniclip compiled or otherwise collected information from 8 Ball Pool to form any sort of data library that would correspond with individual users.

Another factor that some courts have relied on is the "pervasiveness" of the alleged invasion. In Facebook Tracking, the Ninth Circuit held that the plaintiffs had adequately pled a claim for invasion of privacy where they had alleged that Facebook used internet browser plug-ins to track which websites they visited, even after they had logged out of Facebook. 956 F.3d 589, 596 (9th Cir. 2020). Not only did Facebook Tracking involve allegations that Facebook compiled this information into personal user profiles and sold those profiles to advertisers to generate revenue, the Ninth Circuit specifically distinguished the case from other invasion of privacy claims which had been dismissed at the pleading stage because the Facebook Tracking plaintiffs had alleged that Facebook's invasion of privacy continued even after they had ceased using the application. Id. at 606 n.8 (citing cases).

Much like the cases the Ninth Circuit sought to distinguish, Mastel does not allege that 8 Ball Pool continued to view or copy the contents of his Pasteboard after he had closed the application. (See Compl. ¶¶ 22-25.) This case therefore does not present the sort of "pervasive" invasion of privacy that led the court in Facebook Tracking to conclude that the plaintiffs had adequately stated a California constitutional claim for invasion of privacy. See Facebook Tracking, 956 F.3d at 606 n.8.

***9** Finally, some courts have held that the information obtained by the defendant may itself be so sensitive or private that the alleged intrusion alone suffices to state a claim. However, these cases almost always involve information which is clearly more private or sensitive that that at issue in this case. See Hill, 7 Cal. 4th at 40-41 (holding that plaintiffs had stated a claim for invasion of privacy against NCAA based on requirement that athletes provide urine samples under closely monitored conditions, thus implicating "a human bodily function that by law and social custom is generally performed in private and without observers"); Goodman v. HTC America, Inc., 2012 WL 2412070, *15 (W.D. Wash. 2012) (holding collection of continuous geolocation data sufficient under California Constitution because such data may reveal private information such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, union meeting, mosque, synagogue or church, the gay bar and on and on" (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)). Even "highly personal information, including social security numbers, does not 'approach [the] standard' of actionable conduct under the California Constitution and thus does not constitute a violation of" a plaintiff's right to privacy. In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (citing Ruiz v. Gap, Inc., 540 F. Supp. 2d 1121, 1128 (N.D. Cal. 2008)).

The allegations in Mastel's complaint do not approach this standard. Mastel offers only the broad allegation that the 8 Ball Pool application read text that had been copied onto his Pasteboard, which may have included his contact information, addresses for his friends and relatives, or text from messages that he had sent to friends and relatives, depending on what was in his Pasteboard at the time whenever

he opened the application over an eight year timespan. (Compl.¶¶ 22-23.) He does not specify what the content of any of those messages were, what contact information 8 Ball Pool had access to, which friends or relatives' contact information was obtained, or even point to specific communications that he copied from. (See id.) He provides no indication of the sensitivity of the communications at issue other than a conclusory assertion that they were "personal and private." (Id.) Accordingly, even based on the undisputed allegations presented in the complaint, the court has no basis to conclude that any of the information Miniclip allegedly obtained even rises to the level of sensitivity of a social security number, which itself has been held to be inadequate under the California Constitution without some additional unauthorized use or harm. See Ruiz, 540 F. Supp. 2d at 1128.

Mastel points to one case, Opperman v. Path, Inc., in which a federal district court held that iPhone users' personal contact lists could be considered "highly offensive" such that the plaintiff could state a claim for invasion of privacy based solely on allegations that phone applications had accessed the information without permission. See 87 F. Supp. 1018, 1062 (N.D. Cal. 2014). The court finds Opperman to be distinguishable from this case, however. Not only did Opperman involve a claim for intrusion upon seclusion under California common law, rather than a claim under the California Constitution, but the alleged privacy violations at issue were so widespread and pervasive that the Federal Trade Commission and Congress had already "closely scrutinized the practices at issue...because of concerns that the practices were inappropriate." See Opperman v. Path, Inc., 87 F. Supp. 1018, 1062 (N.D. Cal. 2014).

Notwithstanding the authority cited by Mastel, the weight of the case law indicates that his allegations simply do not approach the sort of "egregious" or "highly offensive" conduct which courts have typically permitted to proceed beyond the motion to dismiss stage. See In re iPhone, 844 F. Supp. 2d at 1063; Hill, 7 Cal. 4th at 40-41. The court therefore concludes that Mastel has failed to state a claim against Miniclip for invasion of privacy under the California Constitution. Id. Furthermore, because Mastel seeks to hold Apple responsible based solely on allegations that it knowingly enabled Miniclip's conduct, the court concludes that Mastel has also failed to state a claim for invasion of privacy under the California Constitution against Apple.

***10** The court will therefore dismiss Mastel's second claim for invasion of privacy under the California Constitution.

C. Stored Communications Act

Next, Mastel claims that Miniclip's conduct violated the SCA, which provides a cause of action against a person who "intentionally accesse[d] without authorization a facility through which an electronic communication service is provided" or "who intentionally exceed[ed] an authorization to access that facility; and thereby obtain[ed], alter[ed], or prevent[ed] authorized access to a wire or electronic communication while it [wa]s in electronic storage in such system." 18 U.S.C. § 2701(a). In other words, to state a claim against Miniclip under 18 U.S.C. § 2701(a), Mastel must show that Miniclip "(1) gained unauthorized access to a 'facility' where it (2) accessed an electronic communication in 'electronic storage.' " Calhoun v. Google LLC, -- F. Supp. 3d --, No. 20-CV-05146-LHK, 2021 WL 1056532, *13 (N.D. Cal. Mar. 17, 2021) (quoting Facebook Tracking, 956 F.3d at 608).

It is questionable whether Mastel's iPhone even qualifies as a "facility" under the SCA. See Hildermann v. Enea TekSci, Inc., 551 F. Supp. 2d 1183, 1204 (S.D. Cal. 2008) (noting, without deciding the issue, that it is questionable whether a laptop computer qualifies as a "facility"). Setting this issue aside, however, Mastel's claim fails because text contained in the Pasteboard is not in "electronic storage" for purposes of the SCA. See id. The SCA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17).

Courts interpreting subsection (A) have held that, because this subsection only applies to messages in "temporary, intermediate storage," its coverage is limited to messages that are in transit but which have not yet been delivered to their intended recipient. See Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (citing In re Doubleclick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001)). For instance, subsection (A) may apply to email messages stored on an internet service provider's server pending delivery to the recipient. See Doubleclick, 154 F. Supp. 2d at 511-12. But once the email reaches its intended recipient and is stored on the recipient's laptop, access does not violate the SCA because it is no longer

in "temporary, intermediate storage." See Hilderman, 551 F. Supp. 2d at 1205.

Plaintiff's own complaint indicates that the Pasteboard does not provide "temporary, intermediate storage" of a communication "incidental to the electronic transmission thereof." Id. Pasteboard is merely a tool that allows iPhone users to copy and paste text from one application to another. (Compl. ¶ 11.) As discussed above, while text placed in the Pasteboard may have originated from a previously-sent or previously-received communication (i.e., a text message or email), there is no allegation in Mastel's complaint that Miniclip was somehow able to access the contents of any of Mastel's communications as they were in transit or prior to their delivery to an intended recipient. (See Compl. ¶¶ 10-29.) Mastel's allegations thus does not satisfy subsection (A) of the SCA's definition of "electronic storage." See Hilderman, 551 F. Supp. 2d at 1205.

***11** Nor does accessing text in the Pasteboard fall under subsection (B). Subsection (B) covers storage of communications "by an electronic communication service for purposes of backup protection" of the communication. 18 U.S.C. § 2510(17). Even assuming Apple qualifies as an "electronic communications service," storage of text in the Pasteboard is plainly not for "purposes of backup protection" of any communication. As Mastel himself alleges, text is only stored in the Pasteboard temporarily--as soon as the user copies a new piece of text, the text previously held in the Pasteboard is deleted. (Compl. ¶ 12.)

The court therefore finds that Mastel has failed to allege a plausible violation of the SCA. Accordingly, the court will dismiss Mastel's third claim against Miniclip for violation of the SCA.

D. California Unfair Competition Law

Finally, Mastel claims that Miniclip and Apple's conduct violated the California UCL, which prohibits "any unlawful, unfair, or fraudulent business act or practice...." Clark v. Countrywide Home Loans, Inc., 732 F. Supp. 2d 1038, 1049 (E.D. Cal. 2010) (Wanger, J.) (quoting Hall v. Time, Inc., 158 Cal. App. 4th 847, 849 (4th Dist. 2008)); see also Cal. Bus. & Prof. Code § 17200, et seq. In order to bring a UCL claim, a plaintiff must have UCL standing, which is distinct from Article III standing. See Ehret v. Uber Tech., Inc., 68 F. Supp. 3d 1121, 1132 (N.D. Cal. Sept. 17, 2014) ("[A] federal plaintiff's [Article III] 'injury in fact' may be intangible and need not involve lost money or property...a UCL plaintiff's 'injury in fact' [must] specifically involve lost money or property.") To establish standing under the UCL, a plaintiff "must establish that [he] (1) suffered an injury in fact and (2) lost money or property as a result of the unfair competition." Birdsong v. Apple, Inc., 590 F.3d 955, 959 (9th Cir. 2009) (citing Cal. Bus. & Prof. Code § 17204)).

Mastel has failed to satisfy the UCL's standing requirement because he has not alleged any economic injury as a result of defendants' conduct. In his opposition to Apple's motion to dismiss, Mastel argues that because he alleges that defendants surreptitiously obtained his personal information, he has "suffered a loss in the value of his personal information." (Pl.'s Opp'n to Apple's Mot. to Dismiss at 12 (Docket No. 22).) However, Mastel's complaint never mentions or describes the economic value of his personal information. (See generally Compl.) Numerous courts have held that disclosure of personal information alone does not constitute economic or property loss sufficient to establish UCL standing, unless the plaintiff provides specific allegations regarding the value of the information. See, e.g., In re Yahoo! Inc. Customer Data Sec. Breach Litig., No. 16-MD-02752-LHK, 2017 WL 3727318, *22 (N.D. Cal. Aug. 30, 2017) (rejecting UCL standing to victims of data breach who had failed to allege specific benefit-of-the-bargain losses or out-of-pocket expenses); In re Facebook Privacy Litig., 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011), aff'd 572 F. App'x 494 (9th Cir. 2014) ("A plaintiff's 'personal information does not constitute property under the UCL."); Archer v. United Rentals, Inc., 195 Cal. App. 4th 807, 816 (2d Dist. 2011) (dismissing UCL invasion of privacy claim because "plaintiffs have failed to demonstrate how...unlawful collection and recordation of personal information...translates into a loss of money or property").

All of the cases cited by Mastel are distinguishable because they either relied on allegations of lost cash payments or specific allegations as to the value of the personal information at issue. See In re Yahoo!, 2017 WL 3727318, at **21-22; In re Anthem Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, *30 (N.D. Cal. May 27, 2016); Calhoun v. Google LLC, --F. Supp. 3d--, No. 20-CV-05146-LHK, 2021 WL 1056532, **1-2 (N.D. Cal. Mar. 17, 2021). In Calhoun, for instance, the plaintiffs devoted 50 paragraphs of their complaint to detailing the economic value of their information, how that value had been lost as a result of Google's conduct, and how Google profited by selling their data in a robust marketplace. See Calhoun, Case No. 20-cv-05146, Compl. (Docket No. 1) ¶ 413 ("the unauthorized

disclosure and taking of their personal information which has value as demonstrated by its use and sale by Google. Plaintiffs have suffered harm in the form of diminution of the value of their private and personally identifiable data and content"), ¶¶ 209-58 (describing the "robust market" for the data Google allegedly collected and monetized).

***12** Moreover, Calhoun relied on cases that address Article III standing, which, unlike UCL standing, does not necessarily require plaintiffs to show economic harm. See Plaid, 2021 WL 1721177, at *14 n.8 ("This court disagrees with Calhoun. It rests on four cases that address Article III standing, which is different from UCL standing."). In fact, in one of these cases, while the Ninth Circuit held (in an unpublished memorandum opinion) that the alleged dissemination of the plaintiffs' personal information and loss of "the sales value of that information" sufficed to confer Article III standing, the court expressly held that these allegations did not confer UCL standing because the plaintiffs had "failed to allege that they 'lost money or property.' " See In re Facebook Privacy Litig., 572 F. App'x 494 (9th Cir. 2014). Because Mastel has failed to present any allegations concerning the economic value of the personal information allegedly obtained by defendants, the court will dismiss Mastel's fourth claim against defendants for violations of the UCL.

IT IS THEREFORE ORDERED that defendants' motions to dismiss (Docket Nos. 8, 21) be, and the same hereby are, GRANTED. Dated: July 14, 2021

**All Citations**

Slip Copy, 2021 WL 2983198

**End of Document**