MARC J. ZWILLINGER (*pro hac vice*)
marc@zwillgen.com
JACOB A. SOMMER (*pro hac vice pending*)
jake@zwillgen.com
ZWILLGEN PLLC
1705 N St NW
Washington, DC 20036
Telephone: 202.296.3585

PENELOPE A. PREOVOLOS (CA SBN 87607)
PPreovolos@mofo.com
MORRISON & FOERSTER LLP
425 Market Street
San Francisco, California 94105-2482
Telephone: 415.268.7000
Facsimile: 415.268.7522

Attorneys for Defendant Apple Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

In Re: iPhone/iPad Application Consumer Privacy Litigation

Case No. 5:11-md-02250-LHK

CLASS ACTION

DEFENDANT APPLE'S REPLY IN SUPPORT OF ITS MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT PURSUANT TO RULES 12(B)(1) AND 12(B)(6)

Date: May 3, 2012
Time: 1:30pm
Ctrm: 8, 4th Floor
Judge: Honorable Lucy H. Koh

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

I. INTRODUCTION

The opening paragraph of Plaintiffs' response says all this Court needs to know. In it, Plaintiffs continue to rely on the vague and nonspecific theory that they somehow were injured because the "personal information and data resources of Plaintiffs was an undisclosed and involuntary cost of the use of their iDevice." (Resp. at 1.) This Court has squarely rejected the theory that the iDevices are "'less secure' and 'less valuable' in light of the privacy concerns." (Order at 6.) Because Plaintiffs still do not offer any "particularized example" or explain how any one of them suffered identifiable harm, they again fail to demonstrate Article III standing.

Plaintiffs attempt to salvage these deficient theories by focusing on new statutory claims (under the Stored Communications Act ("SCA") and Wiretap Act) that they hope will automatically confer standing. But their opposition confirms the reason that Plaintiffs omitted these claims from their previous complaint: the alleged conduct does not implicate these statutes, and they do not provide Plaintiffs with a right to relief. Among other things, the SCA does not apply to information obtained from an individual's phone or personal computing device, only to information held in an electronic communication facility — such as emails on an email provider's server. And neither statute applies where Apple is alleged to be receiving information directly from the phones it manufactured, not accessing or "intercepting" communications between iPhone users and third parties.

Aware that they cannot cure the defects with the iDevice class claims detailed in the Court's Order, Plaintiffs change tack and focus on rehashed claims asserted by the so-called "Geolocation Class."[1] These manufactured claims are entirely speculative and fail to set forth a plausible claim that Apple tracked the location of Plaintiffs Gupta or Rodimer (or any other

[1] Plaintiffs suggest that the previous complaint lacked "geolocation" claims, which "have not yet been ruled on by this Court." (Resp. at 3.) But Plaintiffs' Counsel told the Court last May when arguing against a stay pending consolidation: "There was also a story that broke on literally the same day that the Consolidated Complaint was filed, it publicly broke, which dealt with the issue that's been mentioned a few times today regarding the issue of geolocation. *That geolocation issue does exist in the Consolidated Complaint.*" (*See* Zwillinger Decl., Ex. A May 25, 2011 Hr'g Tr. at 40:8-15 (emphasis added).) Moreover, the Court addressed the allegation that Apple's iOS caused iDevices to retain "unencrypted location history files," but held that such speculative allegations of injury do not support Article III Standing. (Order at 9.)

consumer) — and Apple did not. Tellingly, Plaintiffs Gupta and Rodimer do not identify a single piece of geolocation information from their iPhones that supports their claim that Apple "tracked" or "stored" *Plaintiffs'* location data, despite Plaintiffs' specious claim that "anyone" with access to the device could "easily" obtain such files (*e.g.*, AC ¶ 144). Instead, Plaintiffs speculate that Apple *might* be able to "track" them using "data revealing the unique identifiers of *nearby cellular towers and wireless networks*" — *not* data about Plaintiffs or their device. (Resp. at 3-4 (citing AC ¶¶ 138, 144).) As this Court recognized, Plaintiffs' "speculative allegations" that "Apple's platform caused 'users' iDevices to be able to maintain, synchronize, and retain detailed, unencrypted location history files'" are insufficient to support Article III standing. (Order at 9; AC ¶ 137.)

Because the Geolocation Plaintiffs cannot allege *facts* that support their claims, their opposition now asserts that Plaintiffs need "discovery" to "provide . . . details" about "how their private, personal information was stored and transmitted." (Resp. at 12.) But that request only underscores that these claims are entirely speculative and lack any plausible, factual basis. The Geolocation Plaintiffs base their claims entirely on conjecture following reports of a software bug that caused Apple's servers to log and store data, in unintended circumstances, about hot spots and cell towers — *not* data about the iPhone or its user. (*See, e.g.*, ¶¶ AC 137-38, 145, 147-50.) Plaintiffs must do more than mischaracterize news reports and hope that discovery will turn up evidence on their iPhones to support their claims. At a minimum, they must come forward with specific factual allegations that make it *plausible* to conclude that location data linked to them or their iPhones was in fact collected from or stored on their devices (it was not), and then, that they suffered some concrete, identifiable harm from these supposed practices (they did not). In short, Plaintiffs' Geolocation claims fail for precisely the same reasons as in the prior complaint: they fail to allege any plausible or concrete injury for Article III standing, and do not come close to alleging the elements of a legally sufficient claim. Further, all of Plaintiffs' claims fail for numerous additional reasons discussed below.

II. ARGUMENT

A. Plaintiffs Have Not Alleged Injury-in-Fact.

Both classes' injury claims boil down to the allegations that the iDevices: (1) suffered a diminution in value due to the alleged use of personal information (AC ¶ 72(o)); and (2) consumed resources in an unexpected and unwanted way. (AC ¶¶ 118-21.) Yet not one of the allegations Plaintiffs cite in their Response describes a "particularized injury" to any Plaintiff — only abstract harms that this Court has rejected. (*See* Resp. at 9 n.6 (citing AC ¶¶ 30-34, 136-58); Order at 6.) As to diminution in value, Plaintiffs now ask the court to "scan recent headlines" to find that "personal information" should be treated like currency, even as they fail to point to any personally identifying information that Apple collected or disclosed here. (Resp. at 28.) As to resource consumption, the injuries alleged in ¶¶ 170-177 of Plaintiffs' first complaint are *identical* to the injuries alleged in AC ¶ 308(a-h), and again, fail to identify any specific allegation of actual harm to Plaintiffs.[2] Notably, in their 53-page response, Plaintiffs never explain why, if these theories are true, Plaintiff Lalo bought a new device for full value in October 2011 (despite his own claims of diminished value due to data "siphoning"). (*See* Apple Mem. at 2 n.1; AC ¶ 36.) While Mr. Lalo is only one Plaintiff, his purchase of a new iPhone months after filing suit speaks volumes about the lack of harm suffered by *any* of the named Plaintiffs. This Court rejected these damage theories once, and should do so again.

Despite their attempts to repackage their injuries, Plaintiffs have still not identified a single *non-theoretical* injury that impacted any of them, much less harm that is fairly traceable to Apple. (Apple Mem. at 7-8.) Plaintiffs have not, for example, alleged that a particular Plaintiff incurred excess data charges because of anonymous cell tower and Wi-Fi hotspot data being sent to Apple. Nor does any Plaintiff allege that her storage capacity or battery life has been exhausted or that the use of her iPhone was impacted in any other way by the alleged storage or

[2] *See also* Transcript of Proceedings, Sept. 8, 2011, Dkt. 43-1; Beringer Decl., Ex. C. at 13:25-14:3 (identifying "potential damage to the iDevice in the sense that it consumes resources; limited battery and memory capacity; processing power and bandwidth").

collection of data.[3] In short, no Plaintiff has alleged that her device was impaired *at all*. (*See* Apple Mem. at 24.) *Czech v. Wall St. on Demand, Inc*., 674 F. Supp. 2d 1102 (D. Minn. 2009) (damage theory based on consumption of storage is implausible).[4]

In fact, Plaintiffs Gupta and Rodimer (on behalf of the Geolocation class) *concede* that they suffered no harm and base their claims on the far-fetched and theoretical *possibility* that if their iPhones fell into the wrong hands, unspecified data stored on their iPhones "*potentially* subjects [them] to a host of harms, including stalking." (AC ¶ 157 (emphasis added).) But these speculative harms could have occurred only if someone else (1) unlawfully obtained their device, (2) managed to hack into their phone or computer and bypass their password, and (3) was motivated to spend days analyzing complex, indeterminate data about the location of cell towers and Wi-Fi hotspots (not Plaintiffs). (Zwillinger Decl., Ex. B Apple's Q&A on Location Data, AC ¶ 145 n.13.) Not surprisingly, Plaintiffs don't allege that any of this happened, or that such a hypothetical scenario would be fairly traceable to Apple (rather than the third party who obtained the information). Article III requires far more.

B. Plaintiffs Cannot Bring Claims Under the Wiretap Act or the SCA.

Because they cannot identify harm to any named Plaintiff (or anyone), Plaintiffs assert that their late-added SCA[5] and Wiretap Act claims somehow automatically confer standing. (Resp. at 5.) But none of the numerous law firms that drafted Plaintiffs' first consolidated complaint thought to include these claims, and for good reason: neither of these statutes, which target illegal access to email and interception of communications by third parties, apply to routine

---

[3] The Response grossly mischaracterizes the nature of the allegations in the amended complaint. For example, Plaintiffs cite AC ¶¶ 3, 28, 72(f) and 308 as evidence that they sufficiently alleged that they incurred costly wireless data usage. (Resp. at 7.) These paragraphs show no such thing. *See* ¶ 3 (resource usage was of "measurable and of actual value"); ¶ 28 (Plaintiffs were "unaware of the undisclosed costs . . . including the appropriation of their iDevice resources and bandwidth" and "exploitation of their personal information"); ¶ 72(f) ("undisclosed data transmittal costs"); ¶ 308(a) (alleging resource consumption and degradation of performance "including hard drive space, memory, processing cycles, and Internet connectivity").

[4] Plaintiffs' speculative and unsubstantiated "estimate" of the market value of iDevice storage thus cannot rescue these claims. (AC ¶¶ 118-22, 198.)

[5] Plaintiffs have withdrawn the iDevice class's meritless SCA claim against Apple (Count 11), and only the Geolocation class's SCA claim remains. (Resp. at 33 n.30.)

disclosures of data to Apple, advertisers, software developers, or hardware manufacturers, particularly when made by a party to the "communications." The belated addition of these claims is a last-ditch effort to secure standing where no injury exists. Both claims should be dismissed because neither provides standing or states a claim.

1. Personal Computers Are Not Facilities Under the SCA.

Plaintiffs seek to turn the SCA into a far-reaching computer crime statute that creates broad liability for accessing any personal computer or mobile phone. (Resp. at 11.) This effort conflicts with the SCA's text and existing case law, and exceeds Congress's intent to protect communications in storage with *third party* service providers, such as email providers or ISPs.

As detailed in Apple's moving brief, the SCA governs access to electronic communications stored in "facilities," which are computers *operated by* "*electronic communication service[s]*" ("ECS"). (Apple Mem. at 15 (emphasis added).) Contrary to Plaintiffs' assertions, courts have refused to extend the SCA to end users' personal computers because the SCA, on its face, defines "facilities" to mean computers operated by ECS providers that process electronic communications on behalf of others — such as ISPs, bulletin board systems, and web-based email services. *See United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) (holding that a laptop computer is not a facility); *Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 335 (D.D.C. 2011) ("the [SCA] clearly is not triggered when a defendant merely accesses a physical client-side computer and limits his access to documents stored on the computer's local hard drive or other physical media"); *see also In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001) (the SCA does not prohibit websites from placing "cookies" on personal computers because personal computers are not "electronic communication service providers.").[6]

[6] The legislative history is consistent with this reading: "Section 2701(a) generally prohibits any person from intentionally accessing a wire or electronic communication system without authorization or in excess of authorization, and thereby obtaining access to a wire or electronic communication while it is in electronic storage in the system. *An 'electronic mail' service*, which permits a sender to transmit a digital message to the service's facility, where it is *held in storage until the address requests it*, would be subject to Section 2701." H.R. Rep. No. 99-647, 99th Cong. at 63 (1986) (emphasis added).

To extend the SCA far beyond its plain text and legislative history, Plaintiffs rely on cases that do not address the "facility" issue directly or involve email systems administered by businesses for employee communications. *See In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1275 n.3 (C.D. Cal. 2001) (defendant waived argument that a computer was not a facility by raising issue for the first time on reply); *Expert Janitorial, LLC v. Williams*, No. 3:09-CV-283, 2010 U.S. Dist. LEXIS 23080, at *13 (E.D. Tenn. Mar. 12, 2010) (holding computers belonging to a *business* with its *own proprietary email system* may be facilities).[7] Furthermore, *Chance v. Avenue A, Inc.* assumed that Plaintiffs' computers were "facilities" under the SCA, but stated that "[a]lthough this observation of the disputed facts initially works in Plaintiffs' favor, the subsequent implications of this *rather strained interpretation of a 'facility . . .'* are fatal to their cause of action." 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001) (emphasis added). Consistent with Apple's arguments here, *Chance* held that if a user's computer is a facility, the SCA permits any party placing data on the facility to access it because "any communication between the individual computer and the web site [which placed cookies on it] is a communication 'of or intended for' that user" and cannot violate the SCA. *Id.* (*See also* Apple Mem. at 17-18.)[8]

Accepting Plaintiffs' argument would make every personal computer owner an ECS provider, with all the attendant duties and responsibilities of a service provider, including: evidence preservation obligations, 18 U.S.C. § 2703(f); electronic surveillance assistance obligations, 18 U.S.C. § 2511(2); and reporting obligations to the National Center for Missing and Exploited Children, 18 U.S.C. § 2258A. Congress, however, only intended to place such responsibilities on those who offer electronic communication services to third parties.[9]

---

[7] An electronic communications service must have multiple users, as a business does, not one user as a personal computer or smartphone would. 18 U.S.C. § 2510(15) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

[8] Plaintiffs appear to acknowledge that personal computers are *not* "facilit[ies]" under the SCA by citing case law affirming that "[c]ourts have concluded that 'electronic communication service' encompasses internet service providers as well as telecommunication companies whose lines carry internet traffic." (Resp. at 12-13 (citing case).) Unauthorized access to the "facilities" belonging to *those* entities, which plainly provide ECS service, is what the SCA forbids, not unauthorized access to an individual computer or iPhone.

[9] If a personal computer is a "facility through which an electronic communication service is

2. Plaintiffs' SCA Claims Also Fail Because if the Geolocation Data Was in Electronic Storage, Apple Was the Intended Recipient.

Plaintiffs' argument that anonymous geolocation information was in "electronic storage" pending transmission to Apple but was not intended for Apple is a contradiction in terms. "Electronic storage" by definition is a temporary intermediate state that is *incidental* to a transmission to a third party. 18 U.S.C. § 2510(17). If, as Plaintiffs claim, geolocation data was temporarily stored *pending transmission*, the transmission could only be for Apple. As Apple explained in its motion, under either the SCA or the Wiretap Act, an intended recipient is always authorized to access such communications. 18 U.S.C. §§ 2511(2)(d), 2701(c). Here, the crux of Plaintiffs' claim is that Apple obtained the data to create a map of cell towers and Wi-Fi hotspots. (AC ¶¶ 136-38.) Plaintiffs cannot have it both ways: the information is stored temporarily pending transmission to Apple, making Apple the intended recipient, or the information is not in "electronic storage" in the first place. In either case, a claim cannot be brought under the SCA. (*See* Apple Mem. at 16-18.)[10]

C. The Wiretap Act Is Inapplicable to Apple's Alleged Collection of Non-Content Information from iPhones.

Plaintiffs' Wiretap Act claims fail because they do not point to any communications between users and *third parties* that Apple "intercepted," and instead allege that Apple obtained Wi-Fi and cell tower data directly from the iPhones. The Act defines "electronic communication" to be the "transfer of . . . data . . . transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12). The Wiretap Act thus prohibits intercepting an electronic communication that is in the process of being *transmitted* from one location to another, usually between two parties.[11] *See, e.g., Marsh v. Zaazoom Solutions, LLC*,

---

provided," plaintiffs could circumvent the limitations and exceptions to the CFAA, such as the $5,000 damage threshold or exclusion of software-based actions, by asserting an SCA claim for unauthorized access to any personal computer. 18 U.S.C. § 2701(a)(1).

[10] Plaintiffs incorrectly assert that § 2701(c)(2) is inapplicable because "the iPhone customer," not Apple, is the ECS "user." But both can be ECS "users." Apple is a "user" because communications are sent *to* Apple. Section 2701(c)(2) thus bars Plaintiffs' SCA claim.

[11] The Wiretap Act contemplates that communications will usually be between two parties by providing a defense if one party consents. 18 U.S.C. § 2511(2)(d); *Russell v. Am. Broad. Co., Inc.*, No. 94 C 5768, 1995 U.S. Dist. LEXIS 7528, at *4 (N.D. Ill. May 31, 1995) ("[S]ection

No. C-11-0526-YGR, 2012 U.S. Dist. LEXIS 37758, at *53-54 (N.D. Cal. Mar. 20, 2012) (dismissing Wiretap Act claims because "no defendant in this action acquired the information by capturing the transmission of information that was otherwise in the process of being communicated to another party"); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878 (9th Cir. 2002) (for an interception to occur, a communication "must be acquired during transmission, not while it is in electronic storage"). The geolocation data is only alleged to have been sent to or from *Apple*, not a third party. Like the SCA, the Wiretap Act provides that an intended recipient of a communication cannot be liable for intercepting that communication. 18 U.S.C. § 2511(3)(a); *see also* 18 U.S.C. § 2511(2)(d) (providing it is not unlawful for a person to intercept an electronic communication where such person is a party to the communication or one party has consented); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011) (dismissing Wiretap Act claims based on the receipt of information via a cookie because defendant was an intended recipient).

Second, Wi-Fi hotspot and cell tower locations plainly are not "contents," *i.e.*, "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). Plaintiffs seek to expand the Wiretap Act to encompass "intrusive" information — but it is not a catch-all privacy statute. In fact, Congress's 1986 amendments to the Act *eliminated* the phrase "information concerning the identity of the parties to such communication" from the definition of contents.[12] Since then, courts have interpreted "contents" narrowly. Even when (unlike here) personally identifiable information is involved, courts have found the Wiretap Act inapplicable. *See Hill v. MCI WorldCom Commc'ns, Inc.*, 120 F. Supp. 2d 1194, 1196 (S.D. Iowa 2000) (personally identifying information about a customer is not contents); *Jessup-Morgan v. Am. Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (same). Plaintiffs' Wiretap Act

---

2511(2)(d) unambiguously states that it shall not be unlawful for a person to intercept a communication where "'such person is a party to the conversation'" or where 'one of the parties' has consented to the recording.").

[12] Plaintiffs' reliance on *Pharmatrak* and *Gelbard v. United States*, 408 U.S. 41, 51 n.10 (1972), is misplaced because *Gelbard* interpreted the pre-1986 definition of contents. *Nix v. O'Malley*, 160 F.3d 343, 346 n.3 (6th Cir. 1998), is also inapposite because it involved recording voice calls.

claim misconstrues the statute and should be dismissed.

D. Plaintiffs Cannot State a Claim Under CFAA.

1. Plaintiffs' Claims Are Not About Unauthorized Access.

The Geolocation Plaintiffs do not contend that Apple hacked into their iDevices or engaged in any conduct that triggers the CFAA's narrow prohibition on unauthorized access to a computer. To the contrary, their claims are based on the functionality of software contained on iDevices Apple manufactured and sold, which collected basic data about WiFi hotspots and cell towers (*not* the device or user) and sent that data to Apple's servers. (AC ¶¶ 138, 151.) Apple thus did not engage in "unauthorized access" by installing software on phones it manufactured. (AC ¶ 11.) Plaintiffs can no more pursue computer hacking claims against Apple based on the "resources" consumed by the software installed or downloaded to their iPhones than plaintiffs can sue Microsoft any time the latest Windows update takes up space on a computer hard disk. If a computer hacking claim based on "consumption of resources" were viable, any software functionality that was not pre-approved would give rise to a § 1030 claim against a software developer — exactly the outcome Congress intended to avoid when it amended the CFAA in 2001 to protect software design.

2. Plaintiffs Improperly Base Their CFAA Claims on Software Design.

The CFAA no longer permits plaintiffs to bring claims based on the negligent design or manufacture of hardware, software, or firmware. *See* 18 U.S.C. § 1030(g). In their Response, Plaintiffs rely on *In re AOL, Inc. Version 5.0 Software Litig.*, 168 F. Supp. 2d 1359 (S.D. Fla. 2001) and *In re Toys 'R Us Privacy Litig.*, No. 00-CV-2746 MMC, 2001 U.S. Dist. LEXIS 16947 (N.D. Cal. Oct. 9, 2001), which, in turn, relied on the AOL 5.0 cases. But after these cases, Congress *amended* the CFAA in the USA PATRIOT Act of 2001 to preclude just such software-based claims. Congress added a sentence to 18 U.S.C. § 1030(g), which this Court quoted: "No cause of action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware." (Order at 16.)

Moreover, Plaintiffs cannot aggregate their damages to meet the $5,000 statutory minimum. First, Plaintiffs have no damages to aggregate, because the mere occupation of hard

drive space, or bandwidth, does not constitute damages under the CFAA. (*See* Apple Mem. at 24.) *Czech*, 674 F. Supp. 2d at 1102 (damage theory based on mere consumption of storage is implausible). Second, aggregation is generally only allowed where the harm occurs as a result of a single act or a series of acts against the same plaintiff.[13] Here, however, the only act alleged to have caused harm is the release of software, which cannot serve as the basis for aggregation.

3. Plaintiffs Cannot Demonstrate Damage Under the CFAA, and Claims Under 18 U.S.C. § 1030(a)(5) Cannot Be Based on "Loss."

Plaintiffs make separate damage arguments on behalf of each class, but those arguments boil down to theories that this Court has already rejected. The Geolocation Class's latest attempt to put an arbitrary and unsubstantiated price tag[14] on the consumption of resources is insufficient. This Court already found that the same actions alleged in the previous complaint did not interfere with the iDevice's ordinary and intended operation for purposes of injury under Article III standing, much less "damage" under the CFAA. (Order at 19.) As to the iDevice class, Plaintiffs' rehashed arguments about the economic value of their personal information were also rejected by this Court. (*Id.*) Moreover, the alleged collection of "personal information" does not impair the integrity of the data, and any loss of confidentiality is not damage under the CFAA. *See* 18 U.S.C. § 1030(a)(5)(B); *Consulting Prof'l Res., Inc. v. Concise Techs. LLC*, No. 09-1201, 2010 U.S. Dist. LEXIS 32573, at *21 (W.D. Pa. Mar. 9, 2010) ("'damage'" does not "include inappropriate use of data after it has been accessed"), *rep. & rec. adopted*, 2010 U.S. Dist. LEXIS 31489 (W.D. Pa. Mar. 31, 2010).

E. Plaintiffs Do Not State a Claim Under the California Constitution.

Using anonymous location data to build a digital map of "the geographic location of

---

[13] *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004), which Plaintiffs cite, involved intrusions to a single plaintiff's network over a one-year period. *See also La Court v. Specific Media, Inc.*, No. 10-1256-GW(JCGx), 2011 U.S. Dist. LEXIS 50543, at *17 n.4 (C.D. Cal. Apr. 28, 2011) ("It is not clear that, in a civil action not brought by the United States, harm to different persons over a one-year period can be aggregated unless it relates to conduct affecting a single computer."); *but see In re Apple & AT & TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008) (incorrectly relying on the pre-amendment software cases).

[14] Plaintiffs allege their speculative "belief" regarding the amount of storage used, but fail to specify the amount of storage used on any particular Plaintiff's iDevice. (*See* AC ¶ 118.)

cellular towers and wireless networks throughout the United States" is an extraordinary consumer innovation — not an invasion of privacy (much less a serious one) — under the California Constitution. (AC ¶ 137.) Plaintiffs' Response fails to explain how collecting anonymous information about wireless networks and cell towers demonstrates a serious invasion of privacy. Indeed, the data allegedly collected had nothing to do with any consumer, and the Geolocation Plaintiffs do not point to a single piece of geolocation information Apple collected that was in any way linked to the Plaintiffs or their iPhones. Rather, the only location information that the FAC describes is the location of cell towers and hot spots in the United States — information that does not concern the Plaintiffs and is not private in any event. (AC ¶¶ 137-38; Zwillinger Decl., Ex. B.) These allegations do not come close to stating a claim for violation of the right to privacy under the California Constitution. (MID Mot. to Dismiss at 24.)[15]

F. Plaintiffs' CLRA Claim Should Be Dismissed.

Plaintiffs' CLRA claim "necessarily fails" without a sufficient allegation of damage resulting from a defendant's violation of the CLRA. (Order at 14.) As described above, Plaintiffs have not alleged facts demonstrating that any individual Plaintiff sustained any actual damage.

Moreover, Plaintiffs do not dispute that the CLRA does not apply to software. Instead, Plaintiffs argue that their claim is premised on supposed misrepresentations about their iDevices. (Resp. at 36.) But that is not what they pled: as in the prior complaint, their claims are based upon harm allegedly caused by the *software* of certain apps and the operating system designed by Apple. (*See, e.g.*, AC ¶ 161 ("Defendants' software accesses personal information"); ¶ 265 (Apple "designed its iOS 4 software to retrieve and transmit geolocation information").

The CLRA applies only to a "transaction" resulting in the sale of goods or services to a consumer. Cal. Civ. Code § 1770(a). Under the CLRA, Plaintiffs' "original purchase of the iPhone is a *separate transaction*" from the free apps and geolocation features they accessed *after* the original purchase. *Wofford v. Apple, Inc.*, No. 11-CV-0034 AJB NLS, 2011 U.S. Dist. LEXIS

[15] The Mobile Industry Defendants' briefs also refute the iDevice class's constitutional claims, and Apple adopts and agrees with the Mobile Industry Defendants' reply.

129852, at *6 (S.D. Cal. Nov. 9, 2011) (emphasis added).[16] The software, including iOS, that allegedly caused the speculative injury is not a tangible good or service under the CLRA. (Order at 14.) Moreover, Plaintiffs' claim fails because they do not dispute that a CLRA violation may be alleged only by someone who acquires covered goods "by purchase or lease," and the iDevice class challenges only the functionality of *free* apps Plaintiffs received. Cal. Civ. Code § 1716(d).

G. Plaintiffs' Claim Under California's UCL Must Be Dismissed.

1. Plaintiffs Cannot Establish Standing to Bring a UCL Claim.

The FAC does not allege that Plaintiffs have "lost money or property," as required to establish standing under the UCL. Plaintiffs have tried to twist their theory by arguing that had they known about the alleged collection and sharing of their personal information, they would not have purchased or would have spent some unspecified lesser amount for their iPhones. (Resp. at 39.) But that simply dresses up old claims in new clothing: Plaintiffs cannot allege that they relied, when purchasing their iPhones, on the practices of apps they voluntarily downloaded *after* purchase or the operation of software *after* changing settings on their iPhone.

Plaintiffs rely on two cases to support standing: *Kwikset Corp. v. Superior Court* and *Degelmann v. Advanced Medical Optics, Inc*. (Resp. at 39.) Both are inapposite because in both, defendants had made affirmative misrepresentations on product packaging that plaintiffs allegedly saw and relied upon in making their purchasing decisions. *Kwikset*, 51 Cal. 4th 310, 319 (2011). Plaintiffs here *do not* (and cannot) allege that they *saw, read, and relied on* any alleged misrepresentation before they purchased their iPhones. Moreover, Plaintiffs' complaint relies on events that allegedly occurred *after* they purchased their phones — based on downloading free apps or changing the settings on their phones — not misrepresentations on the product label. *Kwikset* and *Degelmann* do not help Plaintiffs here, where no Plaintiff alleges that he relied upon any affirmative misrepresentation at the time he purchased an iPhone.

[16] Contrary to Plaintiffs' assertion, *Kowalsky v. Hewlett-Packard Co.*, No. 10-CV-02176-LHK, (N.D. Cal. Aug. 10, 2011), slip op. (J. Koh), did not discuss the CLRA's applicability to software.

2. Plaintiffs Fail to Allege "Fraudulent," "Unfair," or "Unlawful" Conduct.

Plaintiffs do not dispute that Rule 9(b)'s heightened pleading standard applies to the CLRA and all prongs of the UCL. Plaintiffs cannot satisfy Rule 9(b) with conclusory allegations about a supposed "partial representation" they do not identify, an alleged omission, and their general allegations that they "relied upon" or "were deceived by" representations. (Resp. at 41.) These allegations fall far short of the required "'who, what, when, where, and how' of the misconduct charged." *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1124 (9th Cir. 2009) (citation omitted). The FAC does not allege any specific representation that each Plaintiff was allegedly exposed to; which, if any, representation each Plaintiff allegedly saw, read, and relied on; when or where it was made; who made the alleged representation; or any other specific circumstances regarding Apple's alleged fraud, all of which are required to meet Rule 9(b). These failures are fatal under *Kearns*, 567 F.3d at 1124, as well as *Mazza v. American Honda Motor Co.*, 666 F.3d 581, 596 (9th Cir. 2012) (requiring *exposure to* and *reliance on* alleged representations).

Likewise, Plaintiffs fail to plead a claim under the UCL's "unfairness" prong. Plaintiffs do not dispute that *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006), applies to Plaintiffs' "unfairness" claim under the UCL. (Resp. at 41-42.) But Plaintiffs do not allege the facts required to satisfy that test: (1) a substantial consumer injury; (2) that the injury is not outweighed by countervailing benefits to consumers; and (3) that the injury is one that consumers could not reasonably have avoided. *Camacho*, 142 Cal. App. 4th at 1403.

Indeed, Plaintiffs fail to allege any "consumer injury," much less a substantial one. *See* Section I.A., *supra*. Moreover, Plaintiffs do not even attempt to allege that the claimed injury is not outweighed by the benefits offered by their iPhones and the apps they have chosen to use, or that they were compelled to purchase iPhones or download apps. As this Court previously stated, "Plaintiffs have alternatives to the iDevices," and apps "are nonessential recreational activities." (Order at 11.) Indeed, Plaintiffs concede that "Apple's competitors manufacture, market, and distribute comparable mobile devices that do not collect personal information and track Plaintiffs

without permission . . . ." (AC ¶ 83.)[17]

Plaintiffs rely on their other claims to establish a predicate violation of the "unlawful" prong of the UCL. Because Plaintiffs have failed to allege a violation of any of these laws, their claim under the "unlawful" prong of the UCL should be dismissed with prejudice as well.

H. Apple's Privacy Policy Bars Plaintiffs' Claims.

The iDevice Plaintiffs do not dispute that the iTunes privacy policy governs their claims but argue that a UDID — an alphanumerical serial number — somehow should be considered to be "personal information." (Resp. at 21.) A UDID, however, is exactly what it claims to be, a *Device* Identifier — not a personal identifier. (AC ¶ 2.)[18] The UDID identifies a particular iDevice for the entire life of that device — regardless of whether it is loaned out to another individual, resold, used by different members of a family, or transferred among employees. By definition, a UDID does not identify a unique individual any more than the serial number on a TV set identifies its owner — and, not surprisingly, Plaintiffs do not attempt to cite any instance where their UDID was used to (or able to) identify them. Apple's policies are thus consistent — a UDID is not personal information, and Apple expressly obtained the right to collect and share it.

Because they recognize that the iTunes Privacy Policy permits Apple to obtain the location data at issue here, Plaintiffs now argue that the Privacy Policy somehow does not apply. (Resp. at 11; *see also* McCabe Decl., Ex. G at 1-2, Case No. 10-cv-05878-LHK, ECF No. 143-7 (Privacy Policy provides that Apple "may collect information such as . . . unique device identifier, location . . . so that we can better understand customer behavior and improve our products, services, and advertising.").) Plaintiffs provide no support or explanation for their claim that the

---

[17] Plaintiffs cite one sentence in AC ¶ 333 that encompasses a half-hearted attempt to plead "unfair" conduct "tethered" to a legislatively declared policy. In that sentence, Plaintiffs vaguely reference the CLRA, right to privacy, and unnamed "California statutes," but do not identify *how* any supposed policies are violated by the conduct alleged in the FAC. *See, e.g., Khoury v. Maly's of Cal., Inc.*, 14 Cal. App. 4th 612, 619 (1993).

[18] Contrary to Plaintiffs' reading, regulators, like Apple, have *only* treated device identifiers as personal information when combined with other data. Indeed, the first time the FTC suggested that a UDID should be treated as if it were personally identifiable was in connection with UDIDs collected from children in its recent draft COPPA rulemaking. Comments to FTC, COPPA Rule, Proposed Rule, 76 Fed. Reg. 59804 (Sept. 27, 2011).

Privacy Policy does not apply to them, and indeed, the FAC specifically relies on the Privacy Policy. (AC ¶¶ 77, 78, 315.) Plaintiffs make conclusory allegations that Apple collected "[their] location data," but other allegations in the complaint make clear that, at most, Apple collected anonymous "maps" of surrounding Wi-Fi hot spots and cell towers in a several mile radius — not *Plaintiffs'* location data. Plaintiffs also do not (and cannot) allege that *any* location data was furnished to Apps when location services were off. Plaintiffs' claim that they "withdrew their consent" to have Apple collect "their location data to provide [location services]" is of no consequence here, because Plaintiffs have made no specific allegations that Apple collected *Plaintiffs' location data* or used any data to provide location services to Plaintiffs after they turned off Location Services. (Resp. at 10.)

I. The Limitations on Apple's Duties to Users Contained in Its User Agreements Are Valid and Enforceable.

Plaintiffs' arguments that Apple cannot disclaim liability are misplaced and demonstrate flaws in Plaintiffs' negligence claims beyond those identified in Apple's moving papers. (Apple Mem. at 29-30.)[19] Apple's agreements make clear that it has not assumed a *duty* to review apps prior to purchase — and Plaintiffs have not identified a legal duty that would supplant Apple's contracts. (Order at 13.) While Cal. Civ. Code § 1668 precludes disclaiming liability for negligence if doing so would harm the public interest, it has no impact on contractual provisions that limit the *scope* of any duty owed. As set forth in Apple's motion, Apple's contracts make clear it has not assumed such a duty, thus it has not disclaimed liability improperly. The contract's express provisions stating that App Developers are liable for damages from using Apps is a logical corollary of Apple's clear disclosures that it is *not* undertaking a duty to review Apps.

III. CONCLUSION

For the foregoing reasons, Apple respectfully requests that the Court dismiss all claims against it, with prejudice.

---

[19] In order to avoid repetitive briefing, Apple adopts the arguments with regard to Plaintiffs' trespass, conversion, and common counts claims set forth in the Mobile Industry Defendants' brief, as equally applicable to claims brought against Apple.

Dated: April 5, 2012

ZWILLGEN PLLC

By: /s/ Marc J. Zwillinger
Marc J. Zwillinger

Attorneys for Defendant Apple Inc.