Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 920-3081

*Interim Class Counsel*
(Additional counsel listed on signature page)

**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 |
| | **PLAINTIFFS' RESPONSE IN OPPOSITION TO DEFENDANTS' MOTIONS TO DISMISS** |
| | Hearing Date: May 3, 2012<br>Time: 1:30 PM<br>Courtroom: 8, 4th Floor<br>Judge: Hon. Lucy H. Koh |

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Page(s)**

**FEDERAL CASES**

**CALIFORNIA CASES**

**OTHER CASES**

**FEDERAL STATUTES**



**CALIFORNIA STATUTES**

**OTHER AUTHORITIES**

## PRELIMINARY STATEMENT

> "Your personal privacy should not be the cost of using mobile apps, but all too often it is."

California Attorney General Kamala D. Harris, February 22, 2012.[1]

This case boils down to personal privacy in the form of control over personally identifiable information and data resources. In the First Amended Consolidated Complaint ("FAC"), Plaintiffs have detailed how their personally identifiable information was siphoned from their iDevices without their consent, and they specifically identify the parties responsible for this taking. In particular, Plaintiffs allege that unique device identifiers, along with other data such as real-time location data; the personal name assigned to each Plaintiffs' device (e.g., "Beth's Phone"); gender, age, zip code, and time zone; App-specific activity such as which functions Plaintiffs performed on the Apps; search terms entered; and selections of movies, songs, restaurants or even versions of the Bible, were collected by each Defendant, respectively. Indeed, the personal information and data resources of Plaintiffs was an undisclosed and involuntary cost of the use of their iDevice.

***Defendants' Arguments Fly In The Face Of Well-Pleaded Allegations Of The FAC***

Defendants respond by violating the most fundamental ground rule of a 12(b) motion—they refuse to accept as true the allegations of the FAC. Defendants vainly seek to avoid liability by ignoring the salient factual predicates of the FAC: that the data taken from and about Plaintiffs was personally identifiable, and it was taken without consent or authorization. Contrary to the detailed factual allegations in the FAC, Defendants just repeat their false mantras that all the data collected and shared is anonymous, and that Plaintiffs somehow authorized it. Yet Defendants cannot escape the truth: the data collected by Defendants and at issue in this

[1] Office of the Attorney General, News Release, February 22, 2012, (Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications). *See* Kravitz Decl. Ex A, p. 1. Just as the California Attorney General looks to Apple to protect the privacy of its customers from abuses that may occur via the Apps it offers up in its exclusive App Store, Plaintiffs here look to Apple to fulfill the duties it undertook to safeguard and protect their data.

lawsuit allows Defendants to identify Plaintiffs individually, and associate them with their most private and sensitive activities.

Plaintiffs allege that Defendants' undisclosed tracking of their person, and confiscation of the value of their personal information, violated their rights, caused them economic harm, and unjustly enriched Defendants. All of which was accomplished by the Apple created ecosystem that both harvests Plaintiffs' personal information for its own economic gain, and delivers such data to third party Tracking Defendants that lurk behind the veil, out of sight—and out of mind—of consumers like Plaintiffs. In addition, both Apple and the Tracking Defendants helped themselves to the limited resources of Plaintiffs' iDevices (including memory, bandwidth, and battery life) without ever disclosing their conduct, and without any recompense to Plaintiffs who have paid, and continue to pay, for those resources. These wrongs form the backbone of Plaintiffs' claims. In response, Defendants argue that this is just the way the world works and that, since Plaintiffs purportedly have not been harmed, there can have been no foul.

Fortunately for the hundreds of thousands (if not millions) of iPhone customers whose personal information and geolocation data was improperly collected and used by Apple and the Tracking Defendants, none of Defendants' arguments have merit. The Attorney General of California does not believe that is the way the world should work, and neither do Plaintiffs. And at this stage of the proceeding, where the well-pleaded allegations of the FAC must be taken as true, neither should this Court.

***The Wrongs Alleged In the Complaint Are Actionable***

The FAC sets forth numerous and specific wrongful conduct associated with tangible harms and actionable claims. The Plaintiffs that suffered these harms have been divided into two proposed classes for certification: First, the iDevice Class challenges the collection and disclosure of their personal information, and the unauthorized use of Plaintiffs' iDevice resources and data by all Defendants. Second, the Geolocation Plaintiffs challenge Apple's clandestine tracking of their geolocation information even after Plaintiffs expressly denied Apple permission to do so. While there are certain differences in the claims of each class, Apple's clandestine

tracking, collection and disclosure of personal information is common to both, as is the falsity of Apple's contention that all such data is anonymous.

The claims brought by the iDevice Class were first raised in this consolidated action in an initial consolidated complaint, and were tested by the initial Motions to Dismiss, filed in June 2011 (*Lalo*, Dkt. 145). Plaintiff Arun Gupta filed his Class Action Complaint against Apple (*Gupta v. Apple, Inc.*, Dkt. 1, No. 5:11-cv-02110 (N.D. Cal. Apr. 28, 2011) in April 2011, and it was consolidated into the instant action in May 2011 (*Gupta*, Dkt. 17). As a result of the timing of the consolidation, Defendants' June 20, 2011 Motions and this Court's Order granting Defendants' first motions to dismiss, (Dkt. 8), addressed *only* the allegations made in the initial *Lalo* Consolidated Complaint which were distinct from the claims made in *Gupta*. Plaintiffs thereafter filed the FAC, which now seeks relief on behalf of both the iDevice Class, whose claims are being repleaded from the initial consolidated complaint, and the Geolocation Class, whose claims have not yet been ruled on by this Court.

Thus, while the claims of the iDevice Class have been repleaded to take account of this Court's prior Order, Plaintiffs believe that the Court is generally familiar with those claims and will not restate them here. However, a brief summary of the Geolocation Class claims, that have yet to be addressed by this Court, may be in order. The new claims of the Geolocation Class seek relief for the wrongful collection and misuse of Plaintiffs' location information without consent and the clandestine use of that information for Apple's construction of its digital map. Apple collects personal information and location data from its iPhone customers as part of its plan to develop an expansive database—a digital map—of the geographic location of cellular towers and wireless networks throughout the United States. FAC ¶ 137. Using this digital map, Apple intends to deploy targeted advertisements to mobile phone users. *Id*. To acquire the information needed to construct the digital map, Apple surreptitiously collected geolocation data including, *inter alia*, data revealing the unique identifiers of nearby cellular towers and wireless networks, from its customers' iPhones. FAC ¶ 138. After Plaintiff Gupta filed his original suit, Apple publicly admitted that it had in fact been siphoning geolocation information from its

customers' iPhones without permission, yet claimed that the data collection was the result of a software "bug." FAC ¶ 145. As a result, Apple—or anyone with access to this data—was able to approximate the exact location of thousands, if not millions, of customers, including Plaintiffs Gupta, Rodimer, and the Geolocation Class members. FAC ¶ 144.

Apple's Terms of Serice ("TOS") expressly state that customers may prevent geolocation information from being sent from their iPhones by deactivating the Location Services function on their mobile devices. FAC ¶ 139. The problem for many iPhone users—including the Geolocation Plaintiffs—is that Apple continued to collect and transmit geolocation information from their iDevices even after they withdrew consent to be tracked by turning off their iPhones' Location Services. FAC ¶ 141. Thus, the Geolocation Plaintiffs could not prevent Apple from collecting data about their location, even when they expressly refused to provide their consent to Apple to track them. FAC ¶ 32. This is the factual predicate that gives rise to the claims brought herein on behalf of the Geolocation Class.

Plaintiffs now sufficiently allege, on behalf of both the iDevice Class and the Geolocation Class, that Defendants' surreptitious collection of their private information invaded their constitutional, statutory, and common law privacy rights as well as that Defendants' policies and disclosure practices caused Plaintiffs to suffer actual economic harm. Dismissal is thus improper with respect to any of the Plaintiffs' claims.

## ARGUMENT

### I. THE GEOLOCATION PLAINTIFFS ENJOY BOTH ARTICLE III AND STATUTORY STANDING

Apple's first attack on the Geolocation Plaintiffs is that they lack standing to sue (Apple Br. 6-10). To establish standing, the party invoking the Court's jurisdiction must "demonstrate that it has suffered a concrete and particularized injury that is either actual or imminent, that the injury is fairly traceable to the defendant, and that it is likely that a favorable decision will redress that injury." *Mass. v. E.P.A.*, 549 U.S. 497, 517 (2007). "The injury may be minimal," *Preminger v. Peake*, 552 F.3d 757, 763 (9th Cir. 2008), and "may exist by virtue of 'statutes creating legal rights, the invasion of which creates standing.'" Dkt. 8, "Order" at 5:17–18

(quoting *Edwards v. First Am. Corp.*, 610 F.3d 514, 517 (9th Cir. 2010), cert. granted in part by *First Am. Corp. v. Edwards*, 131 S.Ct. 3022 (2011).) Standing "in no way depends on the merits of the plaintiff's contention that particular conduct is illegal," *Warth v. Seldin*, 422 U.S. 490, 500 (1975), and "does not require . . . an analysis of the merits." *Equity Lifestyle Props., Inc. v. County of San Luis Obispo*, 548 F.3d 1184, 1189 n.10 (9th Cir. 2008).

### A. The Geolocation Plaintiffs' Allegations of Statutory and Constitutional Violations Demonstrate Injury-in-Fact

As this Court stated in its September 20, 2011 Order, invasion of a legal right satisfies the injury requirement for standing where "the constitutional or statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief." Order at 5:17–22 (quoting *Edwards*, 610 F.3d at 517). The Court's reasoning applies with equal force here.

The Geolocation Plaintiffs have standing because they plead violations of their statutory rights under the ECPA, the SCA, and the CFAA. Under clear Ninth Circuit authority, this alone is sufficient to confer injury in fact. *Jewel v. National Security Agency*, 2011 U.S. App. LEXIS 25951, *11 (2011) quoting Lujan v. Defenders of Wildlife, 504 U.S. 555, 578 (1992); *Fulfillment Servs. Inc. v. UPS, Inc.*, 528 F.3d 614, 618-19 (9th Cir. 2008); *Edwards v. First Am. Corp.*, 610 F.3d at 517 ("The injury required by Article III can exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing.'"). In such cases, the "'standing question . . . is whether the constitutional or statutory provision on which the claim rests properly can be understood as granting persons in the plaintiff's position a right to judicial relief.'" *Edwards*, 610 F.3d at 517 (citation omitted).

In its Order, this Court recognized that, "statutory standing under the Wiretap Act does not require a separate showing of injury, but merely provides that any person whose electronic communication is 'intercepted, disclosed, or intentionally used' in violation of the Act may in a civil action recover from the entity which engaged in that violation.'"[2] Order at 8:20–24 (citing

[2] The "Wiretap Act" and "ECPA" are used interchangeably.

18 U.S.C. § 2520(a)). This analysis is in accord with other courts throughout the country, which have routinely found injury-in-fact where a plaintiff alleges violation of a consumer privacy statute with a private right of action. *See, e.g.*, *Graczyk v. West Pub. Co.*, 660 F.3d 275, 278 (7th Cir. 2011) (finding no monetary harm necessary to state a claim under the Driver's Privacy Protection Act, as "Congress has defined the relevant injury under the DPPA as the 'obtain[ment], disclos[ure], or [use]'") (citation omitted); *Klimas v. Comcast Cable Comms., Inc.*, 465 F.3d 271, 275–76 (6th Cir. 2006) (standing exists where plaintiff alleges violations of the Cable Act's privacy provisions, even absent economic harm); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011) (finding standing under the ECPA based solely on allegations of statutory violation). By alleging violations of their federal statutory rights under the ECPA, (FAC ¶¶ 227–233), the Stored Communications Act, (FAC ¶¶ 219–226), and the Computer Fraud and Abuse Act, (FAC ¶¶ 259–276), the Geolocation Plaintiffs have properly alleged injury-in-fact. *See also In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011) ("The Wiretap Act provides that any person whose electronic communication is 'intercepted, disclosed, or intentionally used' in violation of the Act may in a civil action recover from the entity which engaged in that violation. 18 U.S.C. § 2520(a). Thus, the Court finds that Plaintiffs have alleged facts sufficient to establish that they have suffered the injury required for standing under Article III.").

Likewise, the Geolocation Plaintiffs properly pled injury by alleging that Apple infringed upon their rights under the California Constitution. FAC ¶¶ 234–242. Violation of a constitutional provision also creates standing. *Jewel*, 2011 U.S. App. LEXIS 25951 at *4. Article I, Section 1 of the California Constitution provides an "inalienable right[]" to privacy. The California Supreme Court has affirmed that "the Privacy Initiative in article I, section 1 of the California Constitution creates a right of action against private as well as government entities" for its violation. *Hill v. Nat. Collegiate Athletic Ass'n.*, 7 Cal.4th. 1, 20 (1994). Accordingly, the California Constitution's privacy provision "properly can be understood as granting persons in the plaintiff's position a right to judicial relief." *Warth*, 422 U.S. at 500.

### B. The Geolocation Plaintiffs Allege Concrete, Particularized, and Quantifiable Economic Injuries

The Geolocation Plaintiffs also have standing to sue because they allege that Apple's misconduct caused them economic harm. *See Sierra Club v. Morton*, 405 U.S. 727, 733 (1972) ("[P]alpable economic injuries have long been recognized as sufficient to lay the basis for standing, with or without a specific statutory provision for judicial review."). The Complaint alleges several forms of economic injuries. The secret tracking has resulted in a calculable diminution in the value of their iPhones compared to what the Geolocation Plaintiffs paid for, *i.e.*, a phone that does not (FAC ¶¶ 5, 29, 87, 308), as well as costs incurred from wireless data usage. FAC ¶¶ 3, 28, 72(f), 308. These injuries are concrete—they are actual economic damages in amounts to be calculated and proven at trial—and they are particularized, because they are specific to the Geolocation Plaintiffs and others in their position who were tracked without authorization. *See Lujan*, 504 U.S. at 560 n.1 ("By particularized, we mean that the injury must affect the plaintiff in a personal and individual way."). The Geolocation Plaintiffs meet Article III's injury-in-fact requirement because they allege that Apple directly caused them economic damage.

The cases cited by Apple addressing diminution-of-data-value theories are inapposite. The Geolocation Plaintiffs do not claim that Apple's conduct has decreased the value of their geolocation data or other personal information in the Geolocation Class claims. The Geolocation Plaintiffs' claims are thus readily distinguishable from those at issue in *LaCourt v. Specific Media*, No. SACV 10-1256-GW(JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011), where the court held that the plaintiffs lacked standing because they alleged no specific example of economic injury, "but instead offered only abstract concepts, such as 'opportunity costs,' 'value-for-value exchanges,' 'consumer choice,' and 'diminished performance.'" Order at 7:12–15. The Geolocation Plaintiffs, by contrast, do not depend on allegations of diminished personal data value—they allege that Apple illegally invaded their privacy (FAC ¶¶ 219–242, 259–276), decreased the utility and value of their iPhones, (FAC ¶¶ 5, 29, 87, 308), and caused them to incur costly wireless data usage, (FAC ¶¶ 3, 28, 72(f), 308.) Hence, unlike the plaintiffs in

*LaCourt*, the Geolocation Plaintiffs in this case allege that Apple's tracking practices caused them actual, quantifiable injury. FAC ¶¶ 3, 5, 28, 29, 72(f), 87, 308. For these same reasons, Apple's reliance on *Del Vecchio v. Amazon.com Inc.*, No. C11-366-RSL, 2011 WL 6325910 (W.D. Wash. Dec. 1, 2011); *Low v. LinkedIn Corp.*, No. 11-CV-01468-LHK, 2011 WL 5509848 (N.D. Cal. Nov. 11, 2011);[3] *In re JetBlue Airways Corp., Privacy Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y. 2005); and *In re DoubleClick, Inc., Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001), is unavailing, as the diminution-of-data-value theories advanced in those cases do not coincide with the Geolocation Plaintiffs' claims of increased costs and decreased utility.[4]

Moreover, and despite Apple's arguments to the contrary tangible costs incurred and diminished utility represent conventional allegations of injury-in-fact. *See Degelmann v. Adv. Med. Optics, Inc.*, 659 F. 3d 835, 839–40 (9th Cir. 2011) (allegations of overpayment for consumer good sufficed as economic injury, conferring standing); *see also Johnson v. Allsteel, Inc.*, 259 F. 3d 885, 887–88 (7th Cir. 2001) (decrease in value of bargained-for entitlements sufficient to confer standing); *Womack v. Nissan N. Am., Inc.*, 550 F. Supp. 2d 630, 635 (E.D. Tex. 2007) (decreased value of automobile with inflated mileage conferred standing). The Geolocation Plaintiffs allege invasions of privacy and a diminution in the value of their wireless devices sufficient to satisfy statutory and constitutional standing requirements.

### C. The Geolocation Plaintiffs' Claims are Fairly Traceable to Apple

Apple conflates the Complaint's allegations, and ignores that the Geolocation Plaintiffs assert claims *only* against Apple, based *solely* on Apple's conduct, to redress injuries caused *entirely* by Apple. To satisfy Article III's causation requirement, the Geolocation Plaintiffs need only show "a fairly traceable connection between [their] injury and the complained-of-conduct."

[3] Though unmentioned by Apple, this Court acknowledged in *Low* that where—as here—plaintiffs allege violations of the Wiretap Act, no further allegation of injury is necessary to satisfy the constitutional standing requirement. *Id.* at *6 n.1.

[4] Despite Apple's assertions to the contrary, (Apple Br. 7), *Del Vecchio* was not decided on standing grounds, but on the elements of the underlying claims. 2011 WL 6325910, at *2–6. Indeed, the *Del Vecchio* court provided no standing analysis whatsoever beyond restating the Art. III standard. *Id.* at *2. Likewise, the *JetBlue* and *DoubleClick* rulings were based on failure to allege monetary damages required for breach of contract claims, *JetBlue*, 379 F. Supp. 2d at 327, and CFAA claims. *DoubleClick*, 154 F. Supp. 2d at 525.

*Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 103 (1998). Where a plaintiff alleges "invasion of privacy and violation of statutory protections" based on a defendant's publicly acknowledged phone-tracking system, the harm alleged "can be directly linked to" the defendant's conduct. *Jewel v. Nat. Sec. Agency*, Nos. 10-15616, 10-15638, 2011 WL 6848406, at *7 (9th Cir. Dec. 29, 2011). Like the defendant in *Jewel*,[5] Apple publicly acknowledged that it collected geolocation information from iPhone users after they turned their Location Services off. FAC ¶ 145. The Geolocation Plaintiffs' injuries—invasion of constitutional and statutory rights, and economic costs—were the product of that publicly acknowledged tracking program. *See* FAC ¶¶ 136–158. Accordingly, "the harms [Geolocation Plaintiffs] allege[] . . . can be directly linked to" Apple's acknowledged tracking program.[6]

The Geolocation Plaintiffs allege injury-in-fact—economic harm arising from violation of statutory and constitutional privacy rights—traceable to Apple, and redressable through the monetary and injunctive relief sought in this suit. Accordingly, the Geolocation Plaintiffs have standing to sue, and Apple's motion should be denied.

## II. THE GEOLOCATION PLAINTIFFS PROPERLY ALLEGE VIOLATIONS OF THE SCA AND ECPA

Apple attacks the SCA and ECPA claims on four grounds: (1) that the Geolocation Plaintiffs consented to any geolocation tracking, (Apple Br. 18), (2) that iPhones—mobile devices capable of surfing the Internet, sending and receiving emails, playing videos, and streaming music—are not "facilities" for the purposes of the SCA, (*id.* at 15), (3) that geolocation data is not accessed while in "electronic storage" on the iPhone, (*id.* at 16); and that

[5] Because former President George W. Bush had publicly admitted to authorizing the National Security Agency to engage in warrantless wiretapping, and the plaintiff alleged, *inter alia*, Wiretap Act and SCA claims based on that surveillance program, the harms alleged could "be directly linked" to the Defendant National Security Agency's conduct. *Jewel* at *7.

[6] Apple's skewed reading of the Complaint does not change this. Apple claims that "Plaintiffs have not added a *single factual detail* explaining how Apple caused any one of them identifiable harm." Apple Br. 10 (emphasis in original). This ignores that the FAC includes the Geolocation Plaintiffs' additional factual allegations, (FAC ¶¶ 30–34, 136–158), and statutory and constitutional claims against Apple (FAC ¶¶ 219–242, 259–276).

Apple was either a provider or, paradoxically, the intended recipient of the supposedly unintentional geolocation data collection, (*id.* at 17).

### A. The Geolocation Plaintiffs Withdrew their Consent for Apple to Collect their Geolocation Information

Apple asserts that its iTunes Privacy Policy demonstrates that the Geolocation Plaintiffs agreed to allow Apple access to their Geolocation data. Apple Br. 11–12. *But the Geolocation Plaintiffs claims are not implicated by that agreement.* Put simply, Apple cites the wrong agreement. The iTunes Privacy Policy does not control the actions of the Geolocation Plaintiffs, as they simply turned off Location Services on their iPhones. In reality, the operative agreement is the one presented to the Geolocation Plaintiffs when they purchased their iPhones (the "iPhone TOS"), which provides in pertinent part:

> By using any location-based services on your iPhone, you agree and consent to Apple's . . . transmission, collection, maintenance, processing and use of your location data to provide such products and services. *You may withdraw consent at any time by . . . turning off the Location Services setting on your iPhone.*

FAC ¶ 32 (emphasis added). The Plaintiffs plainly allege they withdrew their consent by turning off the Location Service setting (FAC ¶¶ 141, 145, 154, 224, 225), and that despite doing so, Apple continued to collect the data anyway (FAC ¶¶ 141, 142, 224, 225). Given the plain language of its own iPhone TOS, Apple cannot now credibly maintain that the Geolocation Plaintiffs authorized the collection of their information.

### B. iPhones are "Facilities" Within the Meaning of the SCA

Apple first asserts that, "an individual's computer, laptop, or mobile device . . . is plainly not a facility under the SCA." Apple Br. 15–16. Relevant authority shows otherwise. Apple cites only one decision—which does not actually address whether a computer or mobile device is a "facility"—and ignores a wealth of decisions that hurt its case. *See Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001) (holding that the SCA's definition of "facilities" includes personal computers); *see also In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1275 n.3 (C.D. Cal. 2001) ("The court notes, however, that Section 2701 does not require that Plaintiffs' computers be 'communication service providers' only that they be a **facility** through which an

electronic communication service is provided.") (emphasis in original); *Expert Janitorial, LLC v. Williams*, No. 3:09-CV-283, 2010 WL 908740, at *5 (E.D. Tenn. Mar. 12, 2010) (citing *In re Intuit* and holding that "plaintiff's computers on which the data was stored may constitute 'facilities' under the SCA").

In holding that a computer constitutes a "facility," the *Chance* court noted "although the [SCA] was intended to cover such mid-1980s technological facilities as telephone companies, email servers, and bulletin boards, modern technology has placed the personal computer at a focal point of Internet communications." *Chance,* F. Supp. 2d at 1160. "Smartphone" technology used in the iPhone is as central to Internet communications today as the personal computer was when *Chance* was decided ten years ago. "The line between cell phones and personal computers has grown increasingly blurry . . . [i]ndividuals can store highly personal information on their cell phones, and can record their most private thoughts and conversations on their cell phones through email and text, voice and instant messages[]." *United States v. Park*, No. CR 05-375 SI, 2007 WL 1521573, at *6–8 (N.D. Cal. May 23, 2007) (explaining that if cell phones are not afforded the same protections as computers, there could be "far-ranging consequences"). The iPhone is a handheld computing device (in fact, more sophisticated than personal computers of past) and thus qualifies as a "facility" under the SCA.

### C. Apple Accessed Information in "Electronic Storage" on the Geolocation Plaintiffs' iPhones

Apple also contends that, "information that is stored on a user's iPhone cannot be information in 'electronic storage' for purposes of the SCA." Apple Br. 16. This is not true. As Apple acknowledges, the SCA requires a plaintiff to plead facts supporting a finding that location data was temporarily stored pending delivery to an intended recipient. Apple Br 16. That is precisely what Plaintiffs have done. *See* FAC at ¶ 224 (Apple violated the SCA by "collecting *temporarily stored* location data from the Geolocation Plaintiffs after Location Services was turned 'Off.'") (emphasis added). The Geolocation Plaintiffs allege that Apple retrieved information from their iPhones revealing their real-time location information. FAC at ¶¶ 143, 144. If storage in these files were anything other than temporary and regularly

overwritten, the data (constantly updated cell tower and WiFi network information (FAC ¶ 138)), would quickly consume the iPhone's available memory. The Geolocation Plaintiffs have therefore met their pleading burden that the data was accessed while in temporary "electronic storage." *See, e.g., Skaff v. Meridien N. Am. Beverly Hills, LLC*, 506 F.3d 832, 842 (9th Cir. 2007)).

The Geolocation Plaintiffs would need discovery before they can provide additional details about the iPhone's inner workings to ultimately prove their claim. Smartphones utilize highly advanced technology. It would be unrealistic and contrary to the Federal Rules to require the Geolocation Plaintiffs to provide precise, technical details concerning how their private, personal information was stored and transmitted. Nevertheless, the Complaint states a claim because it provides sufficient facts for the Court to draw a reasonable inference that the information accessed by Apple was temporarily stored on Plaintiffs' iPhones prior to transmission.[7]

**D. Apple is neither a "Service Provider" nor an "Intended Recipient"**

Apple asserts that the SCA provides specific exceptions for "conduct authorized: (1) by the person or entity providing a wire or electronic communication service; [and] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c). Apple fails to show that its actions fit either exception.

Simply put, Apple is not an "electronic communication service" ("ECS") provider. "The weight of persuasive authority holds that companies that provide traditional products and services over the Internet, as opposed to Internet access itself, are not 'electronic communication service' providers within the meaning of the ECPA." *Jetblue*, 379 F. Supp. 2d at 307; *see also Dyer v. Nw. Airlines Corps.*, 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) ("Courts have concluded that 'electronic communication service' encompasses internet service providers as

[7] In light of the above, Apple's discussion of *In re DoubleClick* is misplaced. (Apple Br. 17.) The plaintiff in *DoubleClick* alleged that the data files (cookies) at issue were permanently stored on their hard drives, leading the court to conclude, as a matter of law, that the defendants could not have accessed information in temporary "electronic storage." *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d at 512. Here, Plaintiffs specifically allege that their location information was temporarily stored on their iPhones when Apple accessed it without permission.

well as telecommunication companies whose lines carry internet traffic, but does not encompass businesses selling traditional products or services online."). Apple does not provide any Internet or cellular telephone service—it designs and sells the facilities through which consumers use those services. Therefore, the consent protections afforded to ECS providers under § 2701(c)(1) provide it no cover.

Even assuming *arguendo* that Apple qualified as an ECS provider, § 2701(c)(1) does not immunize companies that obtain consent through deception. *See Theofel v. Farey-Jones*, 959 F.3d 1066, 1071-72 (9th Cir. 2003) ("Like the tort of trespass, the Stored Communications Act protects individuals' privacy and proprietary interests. The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage."). The Ninth Circuit held that courts should:

> construe section 2701 in light of these [trespass] doctrines. Permission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances. Section 2701(c)(1) therefore provides no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access.

*Id.* at 1073. Thus, because the Geolocation Plaintiffs allege that Apple obtained consent, if at all, only through deception, Apple cannot avail itself of § 2701(c)(1).

Nor can Apple take advantage of § 2701(c)(2), which exempts conduct authorized by "*the user* of that service" (emphasis added). Confusingly, Apple appears to characterize either itself or the iPhone device itself as the "user" when it argues that "Apple's use of the Plaintiffs' iPhones to store certain data which it later sent back to itself" is "not a §2701 violation." Apple Br. 18. Crucially, Apple ignores that the "user" here is the iPhone consumer (*i.e.*, Plaintiffs Gupta and Rodimer and the Geolocation Class Members), and not Apple (or the iPhone device itself). More to the point, the users of the ECS in this case are the consumers who purchased the iPhone and who specifically withdrew their consent for Apple to collect their personal information, in accordance with Apple's iPhone TOS. *See* Part II.A *supra*. Apple cannot design the iPhone to deceptively transmit private information without consent, and then claim that it is the user and authorize such conduct. To countenance such self-serving behavior would thwart the SCA's very purpose.

### E. Apple Accessed Information on the Geolocation Plaintiffs' iPhones Without Consent

No amount of semantic wrangling can undo the fact that Apple accessed information on the Geolocation Plaintiffs' iPhones without authorization. Apple essentially argues that it did not "access" Plaintiffs' data in the sense contemplated by the SCA. Apple Br. 18-19. But the case Apple cites, *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1271 (N.D. Cal. 2001), turned on the fact that because the plaintiff *voluntarily* transmitted information to defendant, no "unauthorized access" occurred. The instant facts differ materially. Here, Apple accessed—through the deliberate design of its iOS software—information that was temporarily stored on the Geolocation Plaintiffs' iPhones in direct contravention of their express manifestations of intent to not be tracked. FAC ¶ 224. It is of no consequence that Apple did not technically "log-in" (a requirement Apple seemingly attempts to force upon Plaintiffs (Apple Br. 19)) to the Geolocation Plaintiffs' mobile devices without authorization, as one imagines a hypothetical computer hacker might. *See Shefts v. Petrakis,* 758 F. Supp. 2d 620, 635 (C.D. Ill. 2010) (although court ultimately found that access was authorized, defendant employer "accessed" employee plaintiff's information by configuring software to re-route his e-mails to third-party). Thus, Apple's dispute over the meaning of "access" is fruitless.

### F. The Complaint States a Claim under the ECPA

Apple argues that the Geolocation Plaintiffs' ECPA claim fails because geolocation data supposedly is not "content" under the statute and because it was purportedly the intended recipient of the location information. As explained below, neither argument withstands scrutiny.

#### 1. Apple Intercepted the "Contents" of Communications

Re-characterizing the type of information that it gathered from the Geolocation Plaintiffs' iPhones to avoid the ECPA's force, Apple posits that "information about the identities of parties to a communication and other call data *is not content.*" Apple Br. 21. (emphasis in original). That is a red herring. The Complaint alleges that Apple collected real-time location data, information far more intrusive than the identity of a caller and other incidental call data. *See In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless*

*Tel.*, No. 10-2188-SKG, 2011 WL 3423370, at *9 (D. Md. Aug. 3, 2011) ("[R]eal-time location data implicates at least two distinct privacy interests: the subject's right to privacy in his location and his right to privacy in his movement."); *accord In re Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device*, 396 F. Supp. 2d 294, 323 (E.D.N.Y. 2005). Information regarding a person's real-time location is entitled to greater protection than traditional cellular tower and related data. 2011 WL 3423370, at *38 ("[P]recise location data sought here is neither ancillary information collected by service providers in the course of business nor information that is automatically generated or stored incidental to calls.").

Further, "federal wiretap statutes broadly define 'contents.'" *Nix v. O'Malley*, 160 F.3d 343, 346 n.3 (6th Cir. 1998). The "definition encompasses personally identifiable information." *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003). The "contents" of the communications at issue here are "information concerning the substance, purport, and meaning of that communication," because they uniquely identify individuals' real-time locations, which can lead to precise pinpointing of their whereabouts. 18 U.S.C. § 2510(8); (FAC ¶ 143). As a result, Apple cannot escape liability by asserting as a matter of law that it did not intercept the contents of any communication.

2. **Apple was not an Intended Party to the Geolocation Plaintiffs' Communications**

Apple contends that it cannot be liable under § 2511(2)(d)'s consent provision, because it was a "party to the alleged communication." Apple Br. 21–22. Apple claims to be a party because the transmissions it unlawfully intercepted ultimately reached its servers. This cannot be so, as to hold otherwise would mean that any nefarious actor could simply intercept communications and then claim that it was a party to those communications—and thus not liable for its misconduct. Surely the ECPA does not allow for such an absurd result.

Moreover, "[t]he exception [under §2511(2)(d)] requires a party to the communication to consent to the interception and that the interception be without any criminal or tortious purpose." *Chance*, 165 F. Supp. 2d at 1162. Here, the Geolocation Plaintiffs specifically denied Apple access to their location data, thus prohibiting Apple from being a party to these communications.

*See supra* Part II.A.; *see also Pharmatrak*, 329 F.3d at 19-21 (citing *Chance* with approval and holding that "consent should not casually be inferred. Without actual notice, consent can only be implied when the surrounding circumstances *convincingly* show that the party knew about and consented to the interception.") (citation omitted) (emphasis in original). In this case, the FAC makes explicit that the Geolocation Plaintiffs never consented to Apple being a party to the communications at issue. Accordingly, Apple cannot insulate itself from liability through § 2511(2)(d).

## III. THE GEOLOCATION PLAINTIFFS' CFAA CLAIM ADEQUATELY ALLEGES UNAUTHORIZED ACCESS AND THE REQUISITE $5,000 DAMAGE THRESHOLD

Apple contends that because the Geolocation Plaintiffs purportedly agreed to install certain iPhone software updates, they concurrently granted Apple broad authority to manipulate and siphon data from their iPhones. Apple Br. 23. In doing so, Apple ignores the allegation that it retrieved and sent geolocation data from the Geolocation Plaintiffs' iPhones without consent. FAC ¶ 265. It makes no difference, as Apple would have the Court believe, that Apple used the iPhones' software to effectuate these unlawful transmissions. Apple Br. 11-15. Apple misinterprets *In re Am. Online, Inc., Version 5.0 Software Lit.*, 168 F. Supp. 2d 1359 (S.D. Fla. 2001), the only case it cites to support this position. Apple Br. 23. There, the court *affirmed* that AOL could be liable under the CFAA for misconduct perpetrated through its software products. *In re Am. Online, Inc.*, 168 F. Supp. 2d at 1371 ("As an insider, or a person authorized to access the consumers' computer via the installation process of AOL 5.0, AOL allegedly has transmitted damaging information through its 5.0 program . . . As long as the consumers can otherwise satisfy the CFAA's remaining pleading requirements, their claim under § 1030(a)(5)(A) will not be dismissed."). The Geolocation Plaintiffs adequately plead that Apple violated §§ 1030(a)(5)(A), (B), and (C), by accessing and transmitting information from their iPhones, thus causing them to incur losses. FAC ¶¶ 265, 266. Accordingly, Apple's arguments have no merit.

Apple does not dispute, and thus concedes, that if the Geolocation Plaintiffs suffered damages or loss, in the aggregate, they would meet the requisite $5,000 damage threshold under

the CFAA. Apple Br. 24. The only question is whether the Geolocation Plaintiffs have suffered damages or losses as a result of Apple's unlawful conduct. The answer is yes. Under the CFAA, damage means "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). Here, the Geolocation Plaintiffs specifically allege that their iPhones' capacity to store information was diminished as a result of Apple storing their location information without permission. FAC ¶¶ 264, 266, & 275. Thus, the Geolocation Plaintiffs' iPhones have suffered impairment as defined by the CFAA, *Am. Online, Inc. v. Nat'l Health Care Disc., Inc.*, 121 F. Supp. 2d 1255, 1274 (N.D. Iowa 2000) (genuine issue of material fact exists over whether "impairment" has occurred under the CFAA where capacity has been diminished), and their claims should stand.

## IV. THE GEOLOCATION PLAINTIFFS SATISFY THE THREE REQUIREMENTS OF A CALIFORNIA CONSTITUTIONAL PRIVACY CLAIM

Ignoring the allegations in the FAC and misreading applicable case law, Defendants[8] assert that the California Constitution does not apply to the Geolocation Plaintiffs' claims. Apple Br. 30. This is incorrect. The California Constitution provides that "[a]ll people are by nature free and independent and have inalienable rights," including the right to privacy. Cal. Const. Art. I, § 1 (the right to privacy conferred in § 1 is hereinafter referred to as the "Privacy Initiative.") An individual states a claim under the Privacy Initiative where the following three elements are satisfied: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Hill*, 7 Cal.4th at 39-40. Because the Geolocation Plaintiffs satisfy each of the requisite elements, the Court should deny Apple's motion to dismiss.

### A. The Geolocation Plaintiffs Assert Legally Protected Privacy Interests

The Geolocation Plaintiffs pleaded violations of statutory privacy rights, and therefore allege infringement of their legally protected privacy interests including '"conducting personal

[8] Defendant Apple incorporates the Tracking Defendants' arguments against Plaintiffs' claims for violation of the California Constitution, Conversion, Trespass and Common Counts. Apple Br. 30. Accordingly, the Geolocation Plaintiffs respond to the Defendants' California constitutional arguments collectively, as they relate to the Geolocation Class.

activities without observation, intrusion, or interference,' as determined by 'established social norms' derived from such sources as 'the common law' and 'statutory enactment.'" *Hernandez v. Hillsides, Inc.*, 47 Cal.4th 272, 287 (2009) (internal citation omitted).

The ECPA and the SCA are statutory codifications of the Plaintiffs' right to privacy in their electronic devices. *See* S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 1986 WL 31929, 3555 ("The bill amends the 1968 law to update and clarify Federal *privacy protections and standards* in light of the dramatic changes in new computer and telecommunications technologies") (emphasis added).[9] As shown in Section II, *supra*, the ECPA and SCA protect the Geolocation Plaintiffs from Apple's surveillance program, therefore their privacy interests are "legally protected" by "statutory enactment." *Hernandez*, 47 Cal.4th at 287; *cf. Quon v. Arch Wireless Operating Co., Inc.*, 309 F. Supp. 2d 1204, 1210–11 (C.D. Cal. 2004) (denying motion to dismiss plaintiff's Privacy Initiative claim where text messages were disclosed without consent, and plaintiff asserted an SCA claim).[10]

Further, Defendants' attempts to justify their intrusion into the privacy of the Geolocation Plaintiffs' iPhones fail. While disclosure of putative class members' "mere contact information" to a class representative, (*see Pioneer Elecs. (USA), Inc. v. Super. Ct.*, 40 Cal.4th 360, 370 (2007)), and "essentially public information" such as "the general location of a person's residence," is "not surrounded by a legally protected privacy interest," (*Fredenburg v. City of Fremont*, 119 Cal.App.4th 408, 423 (2004)), the continuous tracking of a person's physical location, without permission and in violation of numerous federal statutes, is treated differently. *See In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, 2011 WL 3423370, at *9 ("[R]eal-time location data implicates at least

[9] *See also Suzlon Energy Ltd. v. Microsoft Corp.*, No. 10-35793, 2011 WL 4537843, at *4 (9th Cir. Oct. 3, 2011) ("Congress' primary intent in passing the ECPA was to protect the privacy interests of American citizens"); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002) (noting that the ECPA, which includes the SCA and amended the Wiretap Act, "was intended to afford privacy protection to electronic communications.")

[10] *See also* Section IV, *infra*, establishing a right to privacy in one's location and movement.

two distinct privacy interests: the subject's right to privacy in his location and his right to privacy in his movement.").

**B. The Geolocation Plaintiffs Had a Reasonable Expectation of Privacy**

Apple promised the Geolocation Plaintiffs that it would not track their locations if they disabled the Location Services features of their iPhones. FAC ¶¶ 31, 139. The Geolocation Plaintiffs expressly denied Apple permission to track them by disabling the Location Services feature. FAC ¶¶ 32, 141. Therefore, Apple itself created an environment where Plaintiffs had a reasonable expectation of privacy.[11]

Defendants erroneously contend that the Geolocation Plaintiffs consented to any privacy intrusion. Tracking Defendants ("TD") Br. 25. This argument ignores Apple's promises, both publicly (FAC ¶ 140), and through its iPhone TOS (FAC ¶ 139), that disabling Location Services would prevent Apple from tracking their locations. As Defendants concede, factors such as "advance notice" and the opportunity to consent to the intrusion are relevant to this reasonableness analysis. TD Br. 25 (quoting *Hill*, 7 Cal.4th at 36). The Geolocation Plaintiffs were given "advance notice" and the "opportunity to consent voluntarily to" Apple's surveillance program, and they expressly opted out, as instructed by Apple. FAC ¶¶ 31, 32, 139, 141. Based on its own opt-out mechanism, and Apple's own promises, the Geolocation Plaintiffs had a reasonable expectation of privacy in their geolocation information.

**C. Apple Seriously Invaded the Geolocation Plaintiffs' Right to Privacy**

The question of whether an invasion is serious enough to warrant the Privacy Initiative's protection involves questions of fact inappropriate for resolution on a motion to dismiss. *See Buzayan v. City of Davis*, No. 2:06-CV-01576-MCE-DAD, 2008 WL 4468627, at *7 (E.D. Cal. Sept. 29, 2008) ("While Defendants claim that disclosure of Plaintiffs' personal information does not constitute a 'serious intrusion' for purposes of invoking either constitutional or common law

[11] Additionally, the question of reasonableness is one of mixed law and fact, inappropriate for resolution at the pleadings stage. *See Hill*, 7 Cal.4th at 40. Accordingly, the Court should not decide—without affording Plaintiffs the benefit of discovery, and the determination of the undisputed facts—that the Geolocation Plaintiffs lacked a reasonable expectation of privacy.

privacy concerns, any determination in that regard raises factual issues not appropriate for disposition as a matter of law on the pleadings.") Accordingly, the Court should reject Defendants' argument that its surveillance of the Geolocation Plaintiffs was not, as a matter of law, sufficiently serious.

The allegations in the Complaint show that Apple's surveillance of the Geolocation Plaintiffs was certainly serious. Defendants over-generalize, failing to distinguish between the iDevice Plaintiffs and the Geolocation Plaintiffs and ignoring that the Geolocation Plaintiffs assert claims going far beyond "routine commercial behavior" (*id.* at 26)[12] by alleging violations of federal privacy laws. Apple promised the Geolocation Plaintiffs that they could opt-out of its electronic surveillance program, they followed Apple's opt-out instructions, and Apple tracked them anyway. FAC ¶¶ 31, 32, 139, 141, 143. Accordingly, Apple's invasion of the Geolocation Plaintiffs' privacy was indeed serious.

## V. PLAINTIFFS' CLAIMS ARE NOT FORECLOSED BY APPLE'S AGREEMENTS

### A. Plaintiffs did not Authorize the Disclosure of the Unique Device Identifiers

Apple's argument that consumers authorized Apple to release their unique device identifiers[13] rests on vague, ambiguous and internally inconsistent provisions contained in the Apple iTunes Privacy Policy that not even a sophist could reconcile. The purported authorization is, therefore, wholly inappropriate for inclusion in any contract (much less a consumer contract) and does not bar Plaintiffs claims.

---

[12] Defendants rely on *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal.App.4th 986, 992 (2011), for the proposition that information collected for marketing purposes cannot be a serious privacy invasion. *Folgelstrom*, however, stands for no such proposition—it dealt with the collection of publicly available address information, which is a completely different sort of privacy invasion than continuous surveillance of a person's exact location.

[13] It is important to note that the FAC is not limited to allegations that Apple only disclosed UDIDs. *See e.g.*, FAC ¶ 2 ("The information collected included, but is not limited to: a Plaintiff's precise home and workplace locations and current whereabouts; unique device identifier (UDID) assigned to Plaintiff's iDevice; personal name assigned to the device (e.g. "Beth's phone"); Plaintiff's gender, age, zip code, and time zone; as well as App-specific activity such as which functions Plaintiff performed on the App; search terms entered; and selections of movies, songs, restaurants or even versions of the Bible."). Presumably Apple has waived any argument with respect to the other types of personal information at issue.

The iTunes Privacy Policy (hereafter the "Privacy Policy") purports to distinguish between "personal" and "non-personal information" and sets forth different rules for when it may collect and disclose personal and non-personal information. *See generally* Beringer Decl. in Support of the Tracking Defendants' Motion to Dismiss ("Beringer Decl."), Ex. A, pp. 21-24.[14] Apple defines "personal information" as "data that can be used to uniquely identify or contact a single person." *Id*. at 21. The "unique device identifier" (hereafter "UDID") plainly meets this definition because it can be used to "uniquely identify or contact a single person." FAC ¶¶ 103-105.[15] Further, the Privacy Policy only allows for collection of personal information for limited purposes, and those purposes do not include disclosure to App developers and/or data aggregators for the purpose of identifying and tracking Plaintiffs and other iDevice users. Consequently, the "personal information" provision in Apple's Privacy Policy does not authorize Apple to disclose Plaintiffs' UDIDs to App developers and data aggregators.

Apple claims that it defines non-personal information as "data in a form that does not permit association with any specific individual," Beringer Decl. Ex. A, p. 22, and it argues that the UDID is non-personal information. Apple is incorrect. The UDID allows "direct association" with the individual owner of the phone and the personal data stored therein. In any event, while the Privacy Policy would allow collection of non-personal information for some broader purposes, under any reasonable reading of the privacy policy, those purposes do not include disclosure to App developers and data aggregators for the purpose of tracking iDevice users. Moreover, even if the UDID were "non-personal information" (which it is not), Apple was required to treat it as personal information pursuant to Privacy Policy which states that, "If we do

[14] As noted in Section II., A., *supra*, the iTunes Privacy Policy, the only Agreement upon which Apple relies, is in no way implicated by the claims brought on behalf of the Geolocation Class.

[15] *See also* FTC Commissioner Julie Brill's Speech at Fordham University School of Law, March 2, 2012, "Big Data, Big Issues," at p. 2, http://ftc.gov/speeches/brill/120228fordhamlawschool.pdf, Kravitz Decl. Ex. D, p. 2 ("Given how closely these devices are now associated with each of us — many of us sleep more closely to our cell phones than we do our spouses!**— data that is linked to specific devices through UDIDs, IP addresses, 'fingerprinting' and other means are, for all intents and purposes, linked to individuals**.") (emphasis added).

combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined." Beringer Decl. Ex A, p. 22.

Apple's attempt to classify the UDID as non-personal information is deceptive because it had reason to know that consumers consider the UDID to be personal information ***as defined by Apple*** insofar as it could not only "uniquely identify" a single individual, but it also associates that individual with private information about him or her. Beringer Decl. Ex A, p. 21. Apple therefore violated its own Privacy Policy when it failed to treat Plaintiffs' UDIDs as personal information. *See generally U.S. v. Stuart*, 489 U.S. 353 (1989) ("It is hornbook contract law that the proper construction of an agreement is that given by one of the parties when "that party had no reason to know of any different meaning attached by the other, and the other had reason to know the meaning attached by the first party." quoting Restatement (Second) of Contracts § 201(2)(b) (1981)); *Wash. State Republican Party v. Wash. State Grange*, 2012 U.S. App. LEXIS 1050 (9th Cir. Jan. 19, 2012)(same); *Johnston v. C.I.R.*, 461 F.3d 1162, 1165 (9th Cir. 2006) (same); see also *Farnsworth on Contracts*, § 7.9 (3rd Ed.).

In addition, state and federal regulators consider UDID data to be personal information, particularly where it is combined with other personally identifiable information. The Federal Trade Commission and the Attorneys General of California, and numerous other states, have all acknowledged that "personally identifiable information" includes:

> "[i]ndividually identifiable information from or about an individual [consumer] including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security Number; (f) ***a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual***; or (g) any information that is combined with any of (a) through (f) above."

(emphasis added). *See In the Matter of Microsoft Corporation*, Federal Trade Commission, File No. 012 3240, Docket No. C-4069, Agreement Containing Consent Order, Aug. 8, 2002, pp. 2-3, http://www.ftc.gov/os/caselist/0123240/ microsoftagree.pdf; *accord In the Matter of Eli Lilly and Company, Assurance of Voluntary Compliance and Discontinuance*, Attorneys General of the

States of California, Connecticut, Idaho, Iowa, Massachusetts, New Jersey, New York, and Vermont, p. 7 n.3, http://supplierportal.lilly.com/Home/Mul-ti_State_Order.pdf and http://epic.org/privacy/medical/lillyagreement.pdf.). This Court should likewise find that the definition of "personal information" includes UDIDs and other unique device identifiers.

Moreover, even if the UDID could be interpreted as non-personal information, the Privacy Policy prohibited its collection and disclosure of such data to App developers or data aggregators for their pecuniary benefit. FAC ¶ 101. Under the terms of the Apple Privacy Policy, Apple was authorized to disclose the UDID only for the benefit of the iDevice user—i.e. "so that [Apple] can better understand customer behavior and improve our products, services and advertising" and because "knowing your contact information, product serial numbers, and information about your computer or device helps us register your products, personalize your operating system, set up your MobileMe service, and provide you with better customer service." Beringer Decl. Ex. A, p. 22.

Apple's Privacy Policy is also patently ambiguous because it includes "with equal prominence two different and entirely inconsistent statements." *Payne v. Commercial Nat'l Bank of Los Angeles*, 177 Cal. 68 (1917). On the one hand, Apple states that "Personal Information" is "data that can be used to uniquely identify or contact a single person," (Beringer Decl. Ex. A, p. 21), and on the other hand, Apple insists that the UDID, which can be used to "uniquely identify or contact a single person" is "Non-personal information." *Id*. *Comedy Club, Inc. v. Improv West Assocs.*, 553 F.3d 1277, 1285 (9th Cir. 2009) ("[I]f a contract is capable of two different reasonable interpretations, the contract is ambiguous.") (*quoting Oceanside 84, Ltd. v. Fid. Fed. Bank*, 56 Cal.App.4th 1441, 1448 (1997)).

If there is any doubt about whether UDIDs constitute personal information under the Privacy Policy, this Court should interpret its language against Apple as the drafter of the Privacy Policy. Cal. Civ. Code § 1654 ("In cases of uncertainty not removed by the preceding rules, the language of a contract should be interpreted most strongly against the party who caused the uncertainty to exist."); *Barnes v. Independent Auto. Dealers of Cal. Health and Welfare*

*Benefit Plan*, 64 F.3d 1389, 1393 (9th Cir. 1995) ("We must construe ambiguities in an ERISA plan against the drafter and in favor of the insured."); *Kunin v. Benefit Trust Life Ins. Co.*, 910 F.2d 534, 539-41 (9th Cir. 1990), cert. denied, 498 U.S. 1013, 112 L. Ed. 2d 587, 111 S. Ct. 581 (1990) (adopting the doctrine of *contra proferentum* as federal common law). The same holds true for the definition of "personal information" itself. Apple cannot escape liability by virtue of its own patently ambiguous contract provisions.[16]

**B. Apple Cannot Disclaim Responsibility For Its Privacy Violations**

Apple tries to avoid this lawsuit by arguing that only the third-party App developers, and not Apple itself, violated Plaintiffs' privacy. For safe measure, Apple also contends that it has disclaimed responsibility for the Plaintiffs' claims. Neither argument has merit. It is Apple's conduct (and the Tracking Defendants' conduct) that is the subject of the Amended Complaint, and Apple's purported disclaimers are legally deficient.[17]

1. **Apple's Conduct Precipitated Plaintiffs' Claims**

The FAC alleges that *Apple* itself engaged in wrongful activities, including that *Apple*: "failed to disclose to Plaintiffs that those 'free' apps included third party spyware," FAC ¶ 16; that *Apple* provided tools enabling App developers "to collect Plaintiffs' information, without detection, and send it to third parties," FAC ¶ 16; that *Apple* "created the App store to furnish

[16] Any ambiguity may be resolved by reference to extrinsic evidence. *Willig v. Exiqon, Inc.*, 2012 U.S. Dist. LEXIS 662 (C.D. Cal. Jan. 3, 2012) ("It is true that whenever the meaning of a contract is uncertain or doubtful, evidence of extrinsic circumstances may be received to clarify the intent of the parties in the contractual language which they used."). Determining the credibility of conflicting extrinsic evidence is an issue to be resolved by the trier of fact, and is not appropriate for resolution on a motion to dismiss, particularly in the absence of discovery. *See Heller v. Tuttle & Taylor*, 2008 Cal.App.Unpub. LEXIS 1177, 14-17 (Cal. App. 2d Dist. Feb. 11, 2008).

[17] Apple should also not be permitted to deflect liability by pointing Plaintiffs to non-existent App privacy policies. The California Attorney General, Kamala D. Harris noted that "one recent study found that only 5 per cent of all mobile apps have a privacy policy" and accordingly entered into an agreement with the "leading operators of mobile applications platforms," **including Defendants Apple and Google**, whereby "[t]hese platforms have agreed to privacy principles designed to bring the industry in line with a California law requiring mobile apps that collect personal information to have a privacy policy." Office of the Attorney General, News Release, February 22, 2012, "Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications." See Kravitz Decl. Ex. A.

consumers' private and personally identifiable information, surreptitiously, to third-party advertising and analytics companies," FAC ¶ 25; that *Apple* "intentionally designed its iOS 4 software to retrieve and transmit geolocation information located on its customers' iPhones to *Apple's* servers," FAC ¶ 30.On a motion to dismiss, zero weight should attach to Apple's attempt to create a factual dispute as to whether or not it has engaged in the misconduct alleged in the FAC.

Apple also argues that Plaintiffs' allegations are limited to Apple's role in "policing" App developers. Apple Br. 13. The reality is that Plaintiffs allege that Apple itself failed to keep its promises to protect its customers' personal information. FAC ¶ 16. Moreover, Apple agreed to "police" App developers by representing expressly and by implication, that: "Apple takes precautions—including administrative, technical, and physical measures—to safeguard your personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction," (FAC ¶ 78), and that "Apple requires that proposed Apps go through a rigorous approval process." FAC ¶ 92. Apple thus assumed the role of preventing App developers from accessing personally identifiable information, and cannot now deny its assumed responsibility. See also Attorney General Harris Press Release, Kravitz Decl. Ex A.

### 2. Apple Cannot Disclaim Liability for Harm Arising From Violations of Constitutional and Statutory Law

Plaintiffs have alleged claims funder the California Constitution; the SCA, ECPA and CFAA, CLRA, and UCL. Apple erroneously asserts that its purported general disclaimers exclude these claims, Apple Br. 11-14, but Apple cannot disclaim liability for its constitutional and statutory violations. "All contracts which have for their object, directly or indirectly, to exempt anyone from responsibility for his own fraud, or willful injury to the person or property of another, *or violation of law,* whether willful or negligent, are against the policy of the law." Cal Civ Code § 1668 (emphasis added). "It is now settled—and in full accord with the language of the statute—that . . . under section 1668, "*a party [cannot] contract away liability for* his fraudulent or intentional acts or for his negligent *violations of statutory law*." *Health Net of Cal., Inc. v. Dep't of Health Services,* 113 Cal.App.4th 224, 234 (2003), quoting *Gardner v.*

*Downtown Porsche Audi*, 180 Cal.App.3d 713, 716 (1986) (holding that "section 1688 invalidates a contractual clause that prohibits any recovery for damages (but not equitable relief) for any violation of statutory or regulatory law not made a part of the parties' contractual obligations."); *see also JRS Products, Inc. v. Matsushita Elec. Corp. of Am.*, 115 Cal.App.4th 168 (2004), rehearing denied (Feb. 25, 2005), review denied (May 12, 2004). Accordingly, Apple cannot disclaim liability for Plaintiffs' statutory and constitutional claims.

3. **Apple Cannot Disclaim Liability for Its Own Negligence**

Cal. Civ. Code § 1668 also prevents Apple from disclaiming its own negligence. Although a party may generally disclaim their own negligence without violating § 1668, courts will strike those disclaimers if enforcement would be contrary to public policy. *Blankenheim v. E. F. Hutton & Co*., 217 Cal App.3d 1463, 1472 (1990), review denied (May 3, 1990) ("a contract exempting from liability for ordinary negligence is valid where no public interest is involved and no statute expressly prohibits it."). Exculpatory provisions that involve the public interest, such as those at issue here, are unenforceable. *Tunkl v. Regents of Univ. of Cal.*, 60 Cal.2d 92, 102 (1963) ("the exculpatory provision may stand only if it does not involve 'the public interest.'").

In *Tunkl*, the Court set forth six characteristics typical of contracts affecting the public interest. *Id.* at 98-101; *see also Reudy v. Clear Channel Outdoors, Inc*., 693 F. Supp. 2d 1091 (N.D. Cal. 2010). Apple's iDevices squarely meet each and every one of the *Tunkl* standards: 1) the telecommunications industry is heavily regulated, and protection of consumer privacy on mobile devices was recently the subject of a hearing before the Senate Judiciary Subcommittee for Privacy, Technology and the Law, a Federal Trade Commission Staff Report and a White

House White Paper; [18] 2) iDevices are of great importance to the public;[19] 3) Apple holds itself out as willing to perform this service for any member of the public who seeks it; 4) Apple, the party invoking exculpation, possesses a decisive advantage of bargaining strength against any member of the public who seeks its services; 5) in exercising its superior bargaining power, Apple confronts the public with a standardized exculpatory adhesion contract, and makes no provision whereby a purchaser may pay additional fees and obtain protection against negligence; and 6) as a result of the transaction, the person or property of the purchaser (in this case, Plaintiffs' information) is placed under the control of the seller, subject to the risk of carelessness by the seller or his agent. 60 Cal.2d at 102. In analyzing each of the *Tunkl* factors, it is clear that Apple's iDevices fall within the public interest. *Id.* Because iDevices are now a matter of public importance, Apple's attempts to insulate itself from liability for its own negligence violate public policy, and are invalid as a matter of law.[20]

## VI. THE IDEVICE PLAINTIFFS ENJOY BOTH ARTICLE III AND STATUTORY STANDING

The arguments made in Section I, *supra*, in support of the Geolocation Plaintiffs' standing apply with equal force to the iDevice Class claims for violation of their rights under the

[18] *See* Transcript of Hearing, United States Senate Judiciary Subcommittee for Privacy, Technology and the Law, May 10, 2011; White Paper, Executive Office of the President of the United States, "Consumer Data Privacy in a Networked World: A Framework for Protecting and Promoting Innovation in the Global Digital Economy," January 2012; FTC Staff Report, "Mobile Apps for Kids: Current Privacy Disclosures are Dis*app*ointing," February 2012. Facts contained in public records are considered appropriate subjects of judicial notice *Metro. Creditors' Trust v. Pricewaterhousecoopers, LLP*, 463 F.Supp.2d 1193, 1197 (E.D. Wash. 2006). Plaintiffs do not ask the Court to take judicial notice of a particular fact discussed at the referenced hearing or in the reports, only that the Subcommittee and the reports demonstrate the business is subject to regulatory activity.

[19] The Office of the White House recognizes the public importance of Internet accessibility: "The Internet is integral to economic and social life in the United States and throughout the world…. Networked technologies also spur innovation, enable new business models, and facilitate consumers' and companies' access to information, products, and services markets across the world." The White House White Paper, at p. 5, *supra* n.18

[20] Given the extensive daily use made of iDevices for such activities as banking, purchasing products, gathering information and navigating in automobiles (FAC ¶ 37), the use of iDevices is at least as necessary as a yellow page directory listing or a yacht slip at a harbor. *See e.g. Pelletier v. Alameda Yacht Harbor*, 188 Cal.App.3d 1551, 1555 (1986) (yacht berths), and *McCarn v. Pac. Bell Directory*, 3 Cal.App.4th 173, 180 (1992) (yellow pages listing).

SCA, CFAA, and the California Constitution, Art. I, Sec. 1. and are incorporated herein by reference. In addition, the iDevice Plaintiffs adequately allege the requisites for standing for their CLRA and UCL claims. *See* sections IX and X, *infra*.

The FAC contains far more detailed claims of the concrete and particularized harms suffered by Plaintiffs than the prior complaint and far more than were held sufficient for standing purposes in *Edwards*, 610 F.3d 514 and *Jewel*, 2011 U.S. App. LEXIS 25951. In those cases, the court held that plaintiffs had standing to bring constitutional and statutory claims even though their allegations of harm were far less concrete and particularized than what Plaintiffs allege in the FAC. Moreover, the iDevice Plaintiffs' SCA and state constitutional claims do not rely on an economic theory of personal information to establish injury-in-fact or harm, but rather on the violation of well-established privacy rights.

Of course, the FAC alleges that Plaintiffs suffered economic harm as well. The economic harms include: the quantifiable loss of the value of their bandwidth, memory and battery resources; the difference in value between what Plaintiffs paid for their iDevices and what they were worth had the hidden costs been adequately disclosed; and that the personal data taken from Plaintiffs had economic value to them.

While Plaintiffs recognize the Court's reluctance to find (as previously pleaded) that Plaintiffs' personal data has economic value, recent events warrant a second look. One need only scan recent headlines to find examples of the proposition that personal information is the currency that is exchanged for access to web and mobile services. *See e.g.*, Matt McGee, Google Screenwise: New Program Pays You To Give Up Privacy & Surf The Web With Chrome, February 8, 2012, http://searchengineland.com/google-screenwise-panel-open-110716; and Ari Melber, The Secret to Facebook's IPO Value, The Nation, February 20, 2012, http://www.thenation.com/blog/166388/secret-facebooks-ipo-value. ("Facebook collects its fees in the far more valuable commodity of personal data."). Accordingly, the economic harms

suffered by Plaintiffs further establish Plaintiffs' Article III standing to pursue their claims in this Court.[21]

## VII. THE IDEVICE CLASS STATES A CFAA CLAIM (SEVENTH COUNT)

### A. Damage Or Loss

Under the CFAA, Plaintiffs must plead either "damage" or "loss." 18 U.S.C. § 1030(g). Plaintiffs have adequately alleged both. The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system or information." 18 U.S.C. § 1030(e)(8). Apple impaired the availability of Plaintiffs' iDevice systems by using their memory capacity for its own purposes, *i.e.*, the creation of large location history files (between 10 and 40 megabytes, enough for a dozen songs or photographs) on each device,[22] which Plaintiffs value at approximately 23 cents for each of Plaintiff's iDevices. FAC ¶¶ 117-120. The Tracking Defendants impaired the availability of Plaintiffs' iDevice systems by "surreptitiously including in the App software certain code components" that were not expected, and which, without Plaintiffs' permission, "consumed portions of the 'cache' and/or gigabytes of memory on their devices." FAC ¶ 72(d). Moreover, the Tracking Defendants' conduct will shorten "the actual utility and life of the iDevice batteries." FAC ¶¶ 199-201. *See also, e.g.* FAC ¶ 63(b) and 198 (Defendant Medialets consumed a large amount of storage on the iDevices, as well as bandwidth resources, without authorization or expectation.). This conduct constitutes an impairment of Plaintiffs' systems under Section 1030(e)(8). *See, e.g., I.M.S. Inquiry Mgmt. Sys., Ltd. v.*

[21] Defendants' "prudential" standing argument has no merit. Plaintiffs specifically allege in the FAC that Defendants' conduct was not a standard or legitimate commercial practice. *See e.g.*, FAC ¶ 238.

[22] Apple's contention that, at most, its use of large location files is just "negligent software design" ignores specific FAC allegations that the conduct was intentional. FAC ¶¶ 30, 115, 158, 224. Resolution of a factual dispute over Apple's intent is a matter for summary judgment or trial after discovery, but not for resolution on a motion to dismiss.

*Berkshire Info. Sys., Inc.*, 307 F.Supp.2d 521, 525 (S.D.N.Y. 2004) (sufficient allegations of CFAA damages, despite lack of allegations of physical damage to data).[23]

Apple asserts that this Court should only find that a computer's resources have been damaged if there is "actual impairment of the user's ability to use the service in addition to the loss of storage capacity." Apple Br. 24. However, the law imposes no such requirement, and Apple ignores Plaintiffs' allegations that Defendants have unreasonably consumed memory and capacity of the iDevices, and shortened the battery life. The CFAA does not recognize a *de minimus* or nominal damage exception. *Czech v. Wall St. on Demand, Inc.*, 674 F.Supp.2d 1102, 1116, n.18 (D. Minn. 2009) (citing 18 U.S.C. § 1030(e)(8) (defining damage as "any impairment")).[24]

Defendants also caused Plaintiffs to incur "loss." The CFAA defines "loss" to include "any reasonable cost to any victim...." 18 U.S.C. § 1030(e)(11). Here, Plaintiffs alleged that their personal information is (1) a scarce asset and Defendants' taking of this asset reduced its value (FAC ¶ 188), and (2) a form of currency they may trade, and that Defendants' taking of this data deprived Plaintiffs of the opportunity cost to exchange the data. FAC ¶ 189. *See In re Toys R Us, Inc., Privacy Litig.*, 00-CV-2746, 2001 WL 34517252 at *11 (N.D.Cal. Oct. 9, 2001) (loss adequately alleged where loss entailed the misappropriation of the "economic value" of "personality" because the personal information obtained by defendants could have been sold to

[23] Apple also damaged Plaintiffs' iDevices by allowing Apps that harm the security and integrity of Plaintiffs' personal information. FAC ¶¶ 270, 130, 107(a). *See Expert Janitorial LLC*, 2010 WL 908740 at *8 (noting the legislative history of the CFAA supports conclusion that intentionally rendering a computer system less secure may be considered damage); *Shurgard Storage Centers v. Safeguard Self Storage, Inc.*, 119 F.Supp.2d 1121, 1126-27 (W.D.Wash. 2000) (impairment of integrity of data where data not maintained in a protected state.)

[24] *Czech* does not help Apple. In contrast to the specific and quantified allegations of loss here, the *Czech* court was faced with an allegation that a cell phone had been damaged because unwanted text messages were sent to the phone. *Id*. at 1115. With only "wholly conclusory" allegations in the complaint, a concern that the receipt of every text message, regardless of size, wanted or unwanted, would create liability under the CFAA, and no allegation that Plaintiff's phone was impaired, the court dismissed the allegation. *Id*. at 1114-1118. Apple also cites *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) and *Del Vecchio v. Amazon.com Inc.*, No. C11-366-RL, 2011 WL 6325910 (W.D. Wash. 2011), to support the theory that a small impairment is insufficient. However, in *Creative Computing*, the court, on appeal of a jury verdict, placed no minimum on losses. In *Del Vecchio*, unlike here, the Plaintiffs did not even attempt to quantify the value of their damages.

market researchers for plaintiffs' financial gain). Plaintiffs quantified the value of their privacy, based on a peer-reviewed study, as between $11.33 and $16.58 per improper access. FAC ¶ 72(o). In addition, Defendants' consuming Plaintiffs' iDevice resources and assets constituted a "cost" to them under the ordinary meaning of that term. *See generally eBay v. Bidders Edge, Inc.*, 100 F. Supp. 2d 1058, 1070 (N.D. Cal. 2000) (in the trespass context, even if defendant used only a small amount of eBay's computer system capacity, eBay was deprived of the ability to use that portion).[25]

**B. Plaintiffs Suffered Over $5,000 In Economic Damages In A Year**

In the aggregate, Plaintiffs' losses clearly exceed $5,000 in one year. Plaintiffs alleged economic losses of between $7.98 and $16.58 for personal data (FAC ¶72(o)), bandwidth was taken (FAC ¶198), their iDevices' battery life was shortened (FAC ¶¶197-202), and memory was consumed by Defendants, that is valued at approximately 23 cents per iPhone (FAC ¶275). Thus, this is not a case like *Bose v. Interclick*, No. 10-cv-9183, 2011WL 434517 (S.D.N.Y. Aug. 17, 2011), *In Re Zynga Privacy Litig*., No. 10-cv-4680 JW (N.D. Cal. June 15, 2011) or *LaCourt v. Specific Media,* 2011 WL 1661532, here no specific dollar amounts were alleged.

**C. Though Unnecessary, Plaintiffs Allege An Identifiable Single Act Of Harm**

Defendants wrongly contend that Plaintiffs cannot identify the "single act" of harm by that would allow the aggregation of damages. TD Br. p. 18. Although some earlier courts concluded that a CFAA plaintiff had to satisfy the $5,000 jurisdictional minimum for each "single act or event" resulting in a CFAA violation, the Ninth Circuit—in a case on which Defendants rely—clearly held that "[t]he "damage floor in [CFAA] contains no 'single act'

[25] Plaintiffs also alleged that they have expended money, time and resources in order to remove the unauthorized programs installed on their iDevices (and to therefore identify the locations of the tracking files, the identity of the tracker, and the App affected). FAC ¶¶ 291 & 308(h). The costs expended by Plaintiffs to remediate the negative effects on their iDevices resulting from Defendant's conduct are compensable under the CFAA.

requirement." *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934-35 (9th Cir. 2004).[26]

**D. Defendants Accessed Plaintiffs' iDevices Without Authorization**

Plaintiffs alleged that Defendants access to their iDevices was "without authorization" or "exceeded authorization." *See* 18 U.S.C. § 1030(a)(4), § 1030(e)(6). A Defendant "exceeds authorized access" … "when initial access to a protected computer is permitted *but the access of certain information is not permitted*." *Shamrock Foods Co. v. Gast*, 535 F.Supp.2d 962, 963 (D. Ariz. 2008) (emphasis added). The "voluntary" download of Apps by Plaintiffs does not constitute authorization for unknown and undisclosed third parties to access *anything* on the iDevice or use the iDevice in *any* way for *any* purpose. *In re Apple & ATTM Antitrust Litig.*, No. C 07-5152, 2010 WL 3521965 (N.D.Cal. 2010) does not vitiate the fact that an otherwise authorized person may be held liable for causing damage without authorization. *In re Am. Online, Inc.*, 168 F.Supp.2d 1359. Unlike *In re Apple & ATTM*, where iPhone owners who voluntarily downloaded software cannot be heard to complaint when the software itself caused damage (*id*. at *7), here Plaintiffs allege that while they knowingly downloaded software Apps, they did not authorize the Tracking Defendants' code which, completely unrelated to the functioning of the Apps, allowed the tracking of their whereabouts and the extraction of their personal information. Courts borrow from common trespass principles to analyze CFAA offenses. *Theofel*, 959 F.3d at 1072-1073. Just as "the busybody who gets permission to come inside by posing as a meter reader is a trespasser," *Id*. at 1073, the Tracking Defendants far exceeded any possible authorization that Plaintiffs conceivably gave to mobile *Apps*.

The App disclosures do not save Defendants.[27] Nothing in the disclosure—that information might be collected by third parties—would put a reasonable consumer on notice of

[26] Even if there were a requirement of a "single act" of harm by Defendants, the specific allegations of the scheme would meet this requirement. Where applied, the "same act" requirement has been interpreted to encompass a defendant's act of "releasing for distribution . . . millions of copies of an Internet access product, which, once installed, allegedly caused the damage to computers." *Toys R Us*, 2001 WL 34517252, at *11 (citing *In re Am. Online, Inc.*, 168 F. Supp.2d 1359). The conduct alleged here is akin to the same type and form as alleged in *Toys R US* and *America Online*.

the mechanism and manner by which the iDevice and the Tracking Defendants' code allow a user to be tracked, have the memory on their iDevices used for storage of information on everywhere they have been, or that their iDevices' other resources would be inordinately diminished.[28] To the contrary, Apple represented that "an App may not access information from or about the user stored on the user's iDevice unless the information is necessary for the advertised functioning of the App." FAC ¶¶ 127,110. The Tracking Defendants' conduct grossly conflicted with that representation. FAC ¶ 174.[29]

## VIII. THE IDEVICE CLASS STATES AN SCA CLAIM (COUNT 11) AGAINST THE TRACKING DEFENDANTS[30]

This claim is based on the Tracking Defendants' unauthorized access to Plaintiffs' iDevices, whereby they obtained access to electronic communications while in electronic storage. The electronic data which was improperly accessed by the Tracking Defendants includes, but is not limited to, GPS location data, the phone's unique device identifier, various Plaintiffs' ages, genders, app ID's and passwords, search terms entered, zip codes, etc. *See* FAC ¶¶ 58-64(a)–(g).

---

[27] Defendants cite to the Dictionary.com privacy policy to assert that its "disclosure" is broad because it references third parties that serve advertisements and collect demographic information. TD Br. 6. However, the disclosure cited by Defendants—which applies only to a single App developer—by its terms only applies to "cookies," and Plaintiffs' lawsuit is not based on cookies, but other means of unauthorized tracking and use of storage, memory and bandwidth resources.

[28] *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 582 n.10 (1st Cir.2001) (holding access might be "unauthorized" under the CFAA if it is "not in line with the reasonable expectations" of the party granting permission (internal quotation marks omitted)); *United States v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991) (holding access unauthorized where it is not "in any way related to [the system's] intended function").

[29] The Tracking Defendants also contend the CFAA's legislative history indicates that it is limited to "destructive computer hacking," but not the subsequent use and misuse of the information. TD Br. 19. Actually, the statute was amended in 1994 "to expand the statute's scope to include civil claims challenging the unauthorized removal of information or programs" from a protected computer. *Pac. Aerospace & Electronics, Inc. v. Taylor*, 295 F.Supp.2d 1188, 1196 (E.D. Wash. 2003) (citing *Shurgard Storage Ctrs., Inc.*,119 F.Supp.2d 1121. The cases cited by the Tracking Defendants do not hold to the contrary.

[30] While the SCA claim was initially alleged against both Apple and the Tracking Defendants, Plaintiffs withdraw this claim (Count 11) as to Apple.

### A. iDevices are a "Facility"

The Tracking Defendants argue that the iDevices are not "facilit[ies] through which an electronic communication service is provided." Plaintiffs address this argument in section II.B., *supra*.[31]

### B. Plaintiffs Identified "Electronic Communications" Accessed

The Tracking Defendants contend that Plaintiffs do not allege that there was an electronic communication because they believe Plaintiffs failed to allege a "'transfer' of electronic data that was 'transmitted' from a Plaintiff to any intended recipient." TD Br. 21. This is not correct. Plaintiffs allege that the electronic data was "transmitted to third parties." FAC ¶ 64. These "third parties" are the App developers. As explained below, the Apps were not free to authorize the Tracking Defendants to access these communications.

### C. The Electronic Communication Was In Electronic Storage

The Tracking Defendants argue that Plaintiffs failed to allege that they accessed data while it was in "electronic storage." TD Br. 22. This is not correct. Plaintiffs allege that the Tracking Defendants violated section 2701(a)(1) by accessing data "while in electronic storage by collecting temporarily stored location data from the iDevice Class' iPhones as set forth in paragraphs 58 through 64" of the FAC. FAC ¶ 347. In paragraphs 58-64 of the FAC, Plaintiffs detail further the exact data that was temporarily stored when Defendants accessed it.

[31] The additional cases on which the Tracking Defendants rely to contend that iDevices are not facilities are inapposite, and indeed misleading. *See Crowley v. Cybersource Corp*., 166 F. Supp.2d 1263, 1271 (N.D. Cal. 2001) (Court reserved judgment on this issue, stating: "The Court, however, need not treat this question any further, because the Court finds no unauthorized access to have occurred"); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1077, n.4 (9th Cir. 2004) (did not, as the Tracking Defendants contend, "declin[e] to hold that the SCA protects communications on PCs" TD Br. 21), but rather, in a footnote found that "the substance of plaintiffs' claims is that the defendants improperly accessed [a server with email]"); *Hilderman v. Enea TekSci, Inc.*, 551 F.Supp.2d 1183, 1204 (S.D.Cal. 2008) (Court did not hold that laptop was not facility, but rather, found under the circumstances that the longer term storage on the hard drive did not constitute "electronic storage" because it was neither "temporary" nor "backup protection" which is required by 18 U.S.C. § 2510(17)); *DoubleClick*, 154 F.Supp.2d at 511 (similar to *Hilderman*, court held that "long-term residence [of files] on plaintiffs' hard drives places them outside of [the SCA's] definition of 'electronic storage' and, hence, [the SCA's] protection.")

This Court and others have upheld the sufficiency of far less detailed allegations regarding "electronic storage." In *In re Intuit*, the court rejected a similar defense argument holding that plaintiff's allegation that defendant "accessed data contained in 'cookies' that it placed in Plaintiffs computers' electronic storage" was sufficient to satisfy the liberal requirements of Federal Rules of Civil Procedure, Rule 8. *In re Intuit*,138 F.Supp.2d at 1277. Notably, plaintiff in that case simply alleged "electronic storage" and not "temporarily stored location data." *See, also, In re Toys R US, Inc.*, 2001 WL 34517252 *3 (allegation that data accessed is "incidentally stored in plaintiff's computers while awaiting final transmission to another location" was sufficient).

**D. The Apps Did Not Provide Valid Authorization to the Tracking Defendants**

The Tracking Defendants' final argument is that the Apps "necessarily authorized" the Tracking Defendants "to access Plaintiffs' 'communications' with them...." TD Br. 23. Defendants base this argument on Section 2701(c)(2), which provides that the SCA "does not apply with respect to conduct authorized" by a user of the electronic communications service "with respect to a communication of or intended for that user."[32] This exception to liability does not apply here because Plaintiffs never authorized the Apps to access this particular data. An entry authorized by the plaintiff is not a trespass, but an "assent or willingness would not be effective" if the defendant knew, or should have known, that plaintiff "was mistaken as to the nature and quality of the invasion intended." *Theofel*, 959 F.3d at 1073. Accordingly, there is "no refuge for a defendant who procures consent by exploiting a known mistake that relates to the essential nature of his access." *Id*. at 1073. Here, Plaintiffs have alleged ample facts that would vitiate any purported consent.

[32] The Tracking Defendants also incorrectly contend that Plaintiffs have not alleged that the data was obtained either "without authorization" or in "excess of an authorization." These terms are not defined in the SCA. *Konop*, 302 F.3d at 879 n. 8. As explained in section V.A., *supra*, Plaintiffs adequately allege that Defendants were not authorized to access this data.

## IX. PLAINTIFFS STATE A CLRA CLAIM AGAINST APPLE

The CLRA protects consumers from "unfair methods of competition and unfair or deceptive acts or practices" in connection with the sale or lease of goods and services. Cal Civ. Code §1761(d). The statute provides that it "shall be liberally constructed and applied to promote its underlying purposes, which is to protect consumers against unfair and deceptive business practices…" Cal. Civ. Code § 1760. The statute proscribes a variety of conduct, including "[r]epresenting that goods or services have . . . characteristics, . . . benefits, or quantities which they do not have" (Cal. Civ. Code § 1770(a)(5)), or "[r]epresenting that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another." Cal. Civ. Code § 1770(a)(7). A "consumer" who suffers "any damage" as a result of any method, act, or practice prohibited by Section 1770 of the statute may assert a claim. Cal. Civ. Code § 1780(a). The CLRA defines "goods" to include "tangible chattels bought or leased for use primarily for personal, family, or household purposes." Cal. Civ. Code § 1761(a).

Plaintiffs and members of the iDevice and the Geolocation Classes (the "Classes") are "consumers" within the meaning of the CLRA because they acquired Apple's iDevices for personal, family, or household purposes, (FAC ¶ 313), and the iDevices they purchased qualify as tangible "goods" within the meaning of the CLRA. Apple contends that Plaintiffs and Class Members cannot state a claim under the CLRA because the CLRA does not apply to software (such as free apps, operating systems, or iOS upgrades). Apple Br. 25. However, Plaintiffs and Class Members' CLRA claims are premised on the fact that Apple misrepresented that it designed the iDevices (and exercised tight control over the development and market for Apps to be used on such devices) with adequate safeguards to ensure the privacy and security of their personal information residing on such devices. FAC ¶ 314-317.

In addition, Plaintiffs have alleged that the hardware of the iDevice is inseparable from the operating system (referred to as firmware)—the combination of the two creates the complete user experience. FAC ¶ 11. Indeed, Apple, in its efforts to prevent "jailbraking" of the iPhone firmware has admitted this very fact: "The iPhone firmware is not itself a product; it is a component of the iPhone mobile computing product." FAC ¶ 11 &n.1 (quoting Responsive

Comment of Apple, Inc. to the U.S. Copyright Office, Kravitz Decl. Ex B, p.18). Therefore, the iDevice qualifies as a "good" no less than a laptop or printer qualifies as a "good" under the CLRA; the mere fact that these goods operate in response to (and are useless without) the commands of code or software does not render them outside the ambit of the CLRA. *See e.g.*, Kravitz Decl. Ex C (*Kowalsky v. Hewlett-Packard Company*, No. 10-CV-02176-LHK, N.D. Cal. Aug. 10, 2011, Slip Op. (J. Koh) (court denied motion to dismiss CLRA claims against the manufacturer of a printer that manifested defect in programing of printer firmware)).[33]

Plaintiffs have alleged that Apple violated the CLRA by engaging in unfair and deceptive acts and practices in connection with the sale of iDevices to Plaintiffs. Apple's past and ongoing acts and practices include, but are not limited to, the following material misrepresentations and omissions with respect to the quality of the iDevice and the Apple ecosystem:

- The purchase price of the phone included access to numerous "free apps," when in fact, such apps were not truly free because Apple and the Tracking Defendants obtain Plaintiffs' valuable information assets, and consume their bandwidth and iDevice resources, such as memory storage and battery life, without consent or notice. FAC ¶¶ 8-9, 13, 16-17, 24-29, 197-202, 315-316.

- Plaintiffs could prevent Apple from collecting geolocation data about them by switching the Location Services setting on their iPhones to "Off," when, in fact, Apple continued to track and store location information about them even when Location Services was set to "off." FAC ¶¶ 139-142; 314.

- Apple designed the iDevice to safely and reliably download third-party Apps; the App Store does not permit Apps that "violate our developer guidelines" including Apps containing pornography, Apps that violate a user's privacy, and Apps that hog bandwidth; "Apple takes precautions — including administrative, technical, and physical measures — to safeguard [users'] personal information against loss, theft, and misuse, as well as against unauthorized access, disclosure, alteration, and destruction;" and Apple does not allow an App to transmit data from a user's iDevice to other parties without the user's consent, (FAC ¶ 315), when, in fact, Apple knowingly permits Apps that subject Plaintiffs to privacy exploits and security vulnerabilities to be offered in the App Store. FAC ¶ 316.

[33] This case is easily distinguishable from both *Ferrington* and *Wofford* as well. In *Ferrington*, the court found that software was not a good or service for the purposes of the CLRA. *Ferrington v. McAfee, Inc.*, No. 10-CV-01455-LHK, 2010 WL 3910169 at *14 (N.D. Cal.). Here, Plaintiffs have not based their CLRA claim on software, but rather on the iDevice itself. FAC ¶ 313. Similarly, unlike in *Wofford v. Apple Inc.*, No. 11-CV-0034 AJB NLS, 2011 WL 5445054 at *2 (S.D. Cal.), Plaintiffs have alleged that it was the sale of the iDevices themselves, not the software, that is at issue.

Plaintiffs relied upon and were deceived by these material misrepresentations and omissions. FAC ¶320. They would not have purchased their iDevices and/or would not have paid as much for them, if Apple had disclosed the true facts that it and the Tracking Defendants would surreptitiously obtain personal information from their iDevices, track their activity and geolocation, and consume portions of the "cache" and/or gigabytes of memory on their devices—memory that Plaintiffs paid for the exclusive use of when they purchased their iDevice. FAC ¶ 118-122, 317. Plaintiffs were misled into purchasing a product that did not meet their reasonable expectations. FAC ¶ 318. Given the undisclosed costs imposed by using the iDevice, it was not as useful to Plaintiffs and was not as valuable to them as the price for which they paid for it. FAC ¶ 319. As a proximate and direct result of Apple's misrepresentations, Plaintiffs and Members of the Classes have been injured and suffered damages in that they have purchased products that invade their privacy, render their personal information insecure, consume their valuable device storage and power resources as well as their Internet bandwidth, and are therefore less valuable products than that which they paid.[34] FAC ¶ 321. This damage includes the privacy and economic consequences set forth above, including the purchase price or premium paid for the iDevice. FAC ¶ 322.

## X. PLAINTIFFS STATE A UCL CLAIM AGAINST APPLE

California's Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, et seq., protects both consumers and competitors by promoting fair competition in commercial markets for goods and services. The UCL is "sweeping, embracing anything that can properly be called a business practice and at the same time is forbidden by law." *Cel-Tech Comm'ns, Inc. v. Los Angeles Cellular Tel. Co.*, 20 Cal.4th 163, 180 (1999). A plaintiff has standing to assert a UCL

[34] Unlike *Meyer v. Sprint Spectrum L.P.*, this is not a preemptive suit. 45 Cal.4th 634, 639 (2009). In the instant action, Plaintiffs have alleged actual damages including: (1) that they paid more for the iDevice than they would have had they known of Defendants' actions; and (2) that Defendants consumed bandwidth and memory space that has a discernable value. FAC ¶¶ 79-84, 118-122.

claim if the complaint alleges (1) a loss of money or property, i.e., some form of economic injury; and (2) injury in fact. *Kwikset Corp. v. Super. Ct.*, 51 Cal.4th 310 (2011).

In *Kwikset Corp.*, the California Supreme Court analyzed the economic harm to consumers who are deceived into purchasing products as a result of misrepresentations about the quality of the product:

> For each consumer who relies on the truth and accuracy of a label and is deceived by misrepresentations into making a purchase, the economic harm is the same: the consumer has purchased a product that he or she *paid more for* than he or she otherwise might have been willing to pay if the product had been labeled accurately. This economic harm—the loss of real dollars from a consumer's pocket—is the same whether or not a court might objectively view the products as functionally equivalent.

*Id.* at 329 (2011) (emphasis in original); *accord Degelmann v. Advanced Medical Optics, Inc.*, 659 F.3d 835, 839 (9th Cir. 2011) (where plaintiffs relied on the representation that product would disinfect their contact lenses, and would not have bought it had they known how poorly it actually worked, plaintiffs suffered economic harm under the UCL).

Plaintiffs have standing to bring a claim under the UCL because they were deceived into purchasing a product that did not operate as represented by Apple. The FAC includes extensive allegations concerning how Plaintiffs purchased iPhones ranging from $199 to $399, and included in this purchase price was access to thousands of third party software applications available in Apple's App Store. FAC ¶ 7-8. Apple specifically and intentionally induced the purchase of iPhones by Plaintiffs by offering thousands of ostensibly "free" Apps with the device. FAC ¶¶ 8-9, 13, 16-17, 26. Apple, however, failed to disclose that those Apps included third party spyware that utilized Apple-provided tools to collect Plaintiffs' personal information and send such information to third parties. FAC ¶¶ 16-17. Had Plaintiffs known of Defendants' practices, they would not have purchased iPhones or paid as much for devices that were substantially devalued by such undesirable practices. FAC ¶ 23.

Additionally, Apple's competitors manufacture, market, and distribute comparable mobile devices that do not collect personal information and track Plaintiffs without permission or adequately disclose those material facts. FAC ¶ 83. Plaintiffs and Class Members suffered actual damages as a result of Apples acts and omissions. Specifically, Plaintiffs and other Class

Members suffered monetary losses, i.e. the purchase price of the iDevice, or at a minimum, the difference between the inflated price and the price Apple should have charged for the product. FAC ¶ 332.

**A. Plaintiffs Have Adequately Alleged Fraudulent Conduct**

To establish an unfair competition claim under the "fraudulent" prong, plaintiffs must show that [the] representations were false or were likely to have misled "reasonable consumers." See *Belton v. Comcast Cable Holdings, LLC*, 151 Cal.App.4th 1224, 1241 (2007). "A fraudulent business practice is one which is likely to deceive the public. It may be based on representations to the public which are untrue, and also those which may be accurate on some level, but will nonetheless tend to mislead or deceive. A perfectly true statement couched in such a manner that it is likely to mislead or deceive the consumer, such as by failure to disclose other relevant information, is actionable under the UCL." *McKell v. Washington Mut., Inc.*, 142 Cal.App.4th 1457, 1471 (2006) (citing *Massachusetts Mut. Life Ins. Co. v. Super. Ct.*, 97 Cal.App.4th 1282, 1290 (2002)); *Prata v. Super. Ct.*, 91 Cal.App.4th 1128, 1137 (2001); *Bank of the West v. Super. Ct.*, 2 Cal.4th 1254, 1267 (1992)) (internal citations omitted).

"The fraudulent business practice prong of the UCL has been understood to be distinct from common law fraud. A common law fraudulent deception must be actually false, known to be false by the perpetrator and reasonably relied upon by a victim who incurs damages. None of these elements are required to state a claim for injunctive relief under the UCL." *In re Tobacco II Cases*, 46 Cal.4th 298, 312 (2009) (internal quotations omitted). "This distinction reflects the UCL's focus on the defendant's conduct, rather than the plaintiff's damages, in service of the statute's larger purpose of protecting the general public against unscrupulous business practices." *Id.* "Reliance is proved by showing that the defendant's misrepresentation or nondisclosure was an immediate cause of the plaintiff's injury-producing conduct." *Id.* at 326.

The FAC details extensively how Apple had a duty to disclose the material privacy and security characteristics of the iDevice and its operation within the Apple-controlled ecosystem because it: (i) knew or should have known about such characteristics at the time that Plaintiffs

and members of the Class purchased the product, inasmuch as Apple created the iDevice, the App Store, and reviewed App Store offerings; (ii) had exclusive knowledge of these material facts, which information was not known to Plaintiffs; and (iii) made a partial representation as to the iDevice's integrity in promoting Plaintiffs' privacy and security interests and interests in the reasonably expected utility of their iDevices, but failed to disclose the material fact that the iDevice, the App Store, the Apps, and the entire Apple ecosystem (and system of relationships with developers and Tracking Defendants) was designed to foster the unauthorized taking of and profiting from Plaintiffs' personal information. FAC ¶ 338. Plaintiffs would not have bought the iDevice had they known that the devices would be used for such purposes.

Apple contends that Plaintiffs do not allege facts demonstrating that Plaintiffs relied on any specific misrepresentation or omission to satisfy the "fraudulent prong" of the UCL. Apple Br. 27. However, Plaintiffs specifically allege that they "relied upon Apple's representations with respect to the cost of their iDevices, the availability of 'free' Apps, and the ability to opt-out of geolocation tracking, in making their purchasing decisions, and the omission of material facts to the contrary was an important factor to them." FAC ¶ 76. *See also* FAC ¶¶ 320, 339. At any rate, Plaintiffs are not required "to plead or prove an unrealistic degree of specificity that the plaintiff relied on particular advertisements or statements when the unfair practice is a fraudulent advertising campaign." *In re Tobacco II Cases*, 46 Cal.4th at 306.

**B. Plaintiffs Have Adequately Alleged Unfair Conduct.**

"A business practice is unfair within the meaning of the UCL if it violates established public policy or if it is immoral, unethical, oppressive or unscrupulous and causes injury to consumers which outweighs its benefits." *McKell, 1*42 Cal.App.4th at 1473. To establish an unfair competition claim under the "unfair prong", courts have considered the following factors: (1) the existence of substantial consumer injury; (2) whether the injury is not outweighed by any countervailing benefits to consumers or competition; and (3) whether the injury could not have been reasonably avoided by the consumer. *Camacho v. Auto Club of So. Cal.*, 142 Cal.App.4th

1394, 1403 (2006); *see also Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1044 (9th Cir. 2010).

Plaintiffs allege that Apple's business acts and practices are unfair because they caused injury-in-fact to Plaintiffs and for which Apple has no reasonable and legitimate justification other than to increase, beyond what Apple would have otherwise realized, its market share and revenue from sales of iDevices. FAC ¶ 331-332. In addition, Plaintiffs allege in FAC ¶ 334 that:

> Apple's *modus operandi* constitutes a sharp practice in that it knew or should have known that consumers care about the status and security of personal information and privacy but are unlikely to be aware of and able to detect the means by which Apple was conducting itself in a manner adverse to its commitments and users' interests, through the undisclosed functions of iDevices and Apps and the related conduct of the Tracking Defendants.

Contrary to its contentions (Apple Br. 28), Plaintiff alleged that Apple's conduct offends public policy in California tethered to the CLRA, the state constitutional right to privacy, and California statutes' recognition of the need for consumers to be informed and equipped to protect their own privacy interests such that consumers may make informed decisions in their choices of merchants and other means of safeguarding their privacy. *See* California Civil Code Section 1798.8.

**C. Plaintiffs Have Adequately Alleged Unlawful Conduct**

"Unlawful business acts or practices within the meaning of the UCL include anything that can properly be called a business practice and that at the same time is forbidden by law." *McKell*, 142 Cal.App.4th at 1474 (quoting *Cel-Tech Comm'ns, Inc., supra*, 20 Cal.4th at 180). "A practice is forbidden by law if it violates any law, civil or criminal, statutory or judicially made, federal, state or local." *McKell* at 1474 (citing *Smith v. State Farm Mut. Auto. Ins. Co.*, 93 Cal.App.4th 700, 718 (2001); *Saunders v. Super. Ct.*, 27 Cal.App.4th 832, 838 (1994)). "By extending to business acts or practices which are 'unlawful,' the UCL permits violations of other laws to be treated as unfair competition that is independently actionable.

Apple's conduct is unlawful in that it violated a host of federal and state statutes: the CLRA, CFAA, SCA, and ECPA, as well as the California Constitution Article I, Section I. Each

of these claims, which are fully addressed in Sections VII through X, as well as XII, may serve as a predicate violation of the "unlawful" prong of the UCL.

## XI. PLAINTIFFS STATE A NEGLIGENCE CLAIM AGAINST APPLE

The elements of negligence under California law are: "(a) a legal duty to use due care; (b) a breach of such legal duty; [and] (c) the breach as the proximate or legal cause of the resulting injury." *Evan F. v. Hughson United Methodist Church*, 8 Cal.App.4th 828, 834 (1992) (italics in original).

Plaintiffs allege that Apple owed a duty to Plaintiffs to protect their personal information and data, and to take reasonable steps to protect them from the wrongful taking of their personal information and the wrongful invasion of their privacy. FAC ¶249. This duty arises out of Apple's tight control of the ecosystem—Apple controls what Apps can and cannot transmit to third parties and Apple controls the fact that its customers are kept in the dark about the spying built into its ecosystem. *See* FAC ¶ 19. Apple's control of the user experience includes restrictions, such as blocking consumers from modifying devices or installing non-App-store Apps, and blocking developers and researchers from publicly discussing Apple's standards for App development, and even prohibiting researchers from analyzing and publicly discussing device shortcomings such as privacy flaws. FAC ¶ 123. As a direct consequence of the control exercised by Apple, Plaintiffs and Class Members could not and cannot reasonably review the privacy effects of Apps and must rely on Apple to fulfill its duty to do so. *See* FAC ¶ 124.

Such a degree of control creates a special relationship between Plaintiffs and Apple and imposes common law duties of reasonable care that go well beyond Apple's contractual obligations. *See* FAC ¶ 133; *see also, Kockelman v. Segal*, 61 Cal.App.4th 491, 499 (1998) (An affirmative duty to protect another from harm may arise, however, where a "special relationship" exists…Such a special relationship is typically where the plaintiff is particularly vulnerable and dependent upon the defendant who, correspondingly, has some control over the plaintiff's welfare).

Apple's duties to Plaintiffs are not based on any contractual obligation, but arise as a matter of law because Apple has at all times been aware of the likelihood of harm that would occur should it fail to act reasonably under the circumstances. FAC ¶ 250. *See Applied Equipment Corp. v. Litton Saudi Arabia Ltd.*, 7 Cal.4th 503, 515 (Cal. 1994) ("The law imposes the obligation that 'every person is bound without contract to abstain from injuring the person or property of another, or infringing upon any of his rights.'…This duty is independent of the contract .... '[A]n omission to perform a contract obligation is never a tort, unless that omission is also an omission of a legal duty.'") (citing Sec. 1708, Civ. Code and *Jones v. Kelly*, 208 Cal. 251, 255 (1929) ("The law imposes the obligation that "every person is bound without contract to abstain from injuring the person or property of another, or infringing upon any of his rights."). As a result, Apple has an independent duty to avoid reasonable harm to others that it reasonably foresees might be harmed by those actions.

Apple also undertook duties to Plaintiffs through its representations that it takes Plaintiffs' privacy seriously, and reviews all Apps for suitability and adherence with its policies. *See* FAC ¶ 125-130; *Schwartz v. Helms Bakery Ltd.*, 67 Cal.2d 232, 238 (1967) ("[A]lthough one individual need do nothing to rescue another from peril not of that individual's own making, nevertheless, '(h)e who undertakes to do an act must do it with reasonable care'"); *Delgado v. Trax Bar & Grill*, 36 Cal.4th 224, 250 (2005) (A defendant's undertaking will support the finding of a duty to another where the defendant's action increased the risk of harm to another, or the other person reasonably relied upon the undertaking to his or her detriment). Apple failed to satisfy its own commitments and, further, failed to satisfy even the minimum duty of care to protect Plaintiff and Class Members' personal information, privacy rights, and security. FAC ¶ 131-135, 253-254.

Plaintiffs have alleged that Apple's breach of its duties proximately caused Plaintiffs' highly personal information (including location information) to become exposed to it and to third parties, without Plaintiffs' consent and authorization. Contrary to Apple's contentions (Apple Br. 30), these allegations of harm are sufficient to state a claim for negligence. *See Claridge v.*

*RockYou, Inc*., 785 F.Supp.2d 855, 866 (N.D. Cal. 2011) (plaintiff's allegations that he was injured by defendant's actions in permitting the unauthorized and public disclosure of his personally identifiable information, which had some unidentified but ascertainable value, are sufficient to allege an actual injury for a negligence claim).

Plaintiffs alleged that such harm was foreseeable for a host of reasons, including that Apple (1) internally treats information such as users' device ID (UDID) as personally identifiable information because when combined with other data, such as geolocation data it personally identifies the user of the iDevice (FAC. ¶ 102-105); (2) intentionally chose to not provide Plaintiffs with any means to disable the iDevice's UDID from being tracked or to restrict access to the UDID (FAC. ¶ 106); and (3) amended its Developer Agreement to specifically prohibit Apps from sending private information to third parties without express consent from the user (although it never actually enforced the change). FAC. ¶ 110.

## XII. THE IDEVICE PLAINTIFFS STATE A CLAIM FOR VIOLATIONS OF THEIR CONSTITUTIONAL RIGHTS TO PRIVACY UNDER THE CALIFORNIA CONSTITUTION (COUNT FOUR)[35]

The iDevice Plaintiffs allege violations of their rights under the Privacy Initiative, Art. 1, §1 of the California Constitution, arising out Defendants' unauthorized access to the geolocation histories and other sensitive personal information about them that was stored in Plaintiffs' iDevices and/or obtained through Apps that Plaintiffs used via their iDevices. First, Plaintiffs have a legally protected privacy interest in their movements and location. *In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel.*, No. 10-2188-SKG, 2011 WL 3423370, at *13 ("… a person has a reasonable expectation of privacy in his aggregate movement over a prolonged period of time."). See also *U.S. v. Jones*, 132 S.Ct. 945, 955 (2012) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.") (J.Sotomayor, concurring). Such GPS data invariably may

[35] In addition to the argument made here, Plaintiffs incorporate the arguments made in Section IV., *supra*.

disclose trips, "the indisputably private nature of which takes little imagination to conjure: 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." *Id*. (*quoting People v. Weaver*, 12 N.Y.3d 433, 441-442, 909 N.E.2d 1195, 1199 (2009).[36]

Courts have already recognized that GPS tracking via smartphones, like the iDevices here, is even more intrusive than the GPS tracking of vehicles. *See In re Application*, , 2011 WL 3423370, at *12 ("While a vehicle may as a matter of fact remain within public spaces during the tracking period…, it is highly unlikely—indeed almost unimaginable—that a cell phone would remain in public spaces.").

In addition to the wealth of information about Plaintiffs' familial, political, professional, religious, and sexual associations that the Tracking Defendants could glean from access to the geolocation histories that Apple surreptitiously stored on their iDevices, the Defendants also obtained sensitive personal information about Plaintiffs when they used Apps, including their age, gender, sex, birthdate, media viewing habits, App activity, and zip code—all of which were associated with Plaintiffs individually by access to their device's UDID, and other identifying information. FAC ¶¶ 58-64.

Second, Plaintiffs reasonably expected that they had a right to privacy for the data on their phones, as well as their location and movement. Plaintiffs alleged that, based upon Apple's representations, they did not expect or believe that Apple would collect or disseminate their location information. FAC ¶¶ 34, 155, 172, 173, 177, 189. Nor was there any notice that the Apps would share sensitive personal information with third parties such as the Tracking

[36] Under California law, it is illegal to use an electronic tracking device to determine the location or movement of a person. *See* Cal. Penal Code §637.7. While §637 criminal liability is expressly limited to a prohibition on attaching devices to a vehicle or other movable thing, the same privacy interest in movement and location that is protected by §637 is implicated here. However, the tracking by Defendants here was even more pervasive than merely tracking an automobile, because iDevices are kept predominantly on or near their owner, and often are held in the privacy of their homes. *See In the Matter of an Application*, 2011 WL 3423370, at *12 (distinguishing GPS tracking of a phone from GPS tracking of vehicles, because vehicles largely remain in public spaces while cell phones are ordinarily on a person).

Defendants here. FAC ¶¶ 173, 245. Indeed, there was no way for Plaintiffs realistically to even know of the existence of the Tracking Defendants, let alone be aware of their conduct. And even if they could have learned of the Tracking Defendants' conduct, there was no way for Plaintiffs to curtail it.

Equally, Plaintiffs' allegations in their Amended Complaint satisfy the reasonable expectations test because their subjective expectations conformed to objective social norms. To assess the reasonableness of a claimant's expectations, a court must consider the customs, practices and physical setting surrounding the disputed acts, placing particular emphasis on any notice provided or consent obtained. *Leonel v. Am. Airlines, Inc*., 400 F.3d 702, 712 (9th Cir. 2005). *See also Hill*, 7 Cal.4th at 36 ("customs, practices, and physical settings surrounding particular activities may create or inhibit reasonable expectations of privacy"). "A reasonable expectation of privacy is an objective entitlement founded on broadly based and widely accepted community norms." *Hill*, 7 Cal.4th at 37. Societal norms simply do not condone the surreptitious collection of geolocation and sensitive personal—and personally identifiable—data that was collected by Defendants here. Even Justice Alito, who was most wary of finding an invasion into an individual's expectation of privacy in *U.S. v. Jones*, 132 S.Ct. at 964 had no trouble stating that "long term GPS monitoring . . . impinges on expectations of privacy." (J. Alito, concurring). Because Plaintiffs have alleged that they had reasonable expectations of privacy with regard to their location information and the other personal information on their phones, and because their expectations conformed to objective social norms, Defendants' motion to dismiss must be denied.

Finally, the extraordinary amount of current regulatory activity more than establishes the serious nature of Defendant's conduct, and that serious privacy interests of Plaintiffs have been–and continue to be–compromised,[37] all without Defendants identifying any countervailing interest.

[37] See IV and V.B.3., *supra*.

## XIII. PLAINTIFFS STATE A CLAIM FOR TRESPASS TO CHATTELS

A claim for trespass to chattels in California "'lies where an intentional interference with the possession of personal property *has proximately caused injury.*'" *Intel Corp. v. Hamidi*, 30 Cal.4th 1342, 1350 (2003) (quoting *Thrifty-Tel, Inc. v. Bezenek*, 46 Cal.App.4th 1559, 1566 (1996) (italics added)). To establish a claim of trespass to chattels, a plaintiff must show that "(1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff." *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp.2d at 1069-70. Harm may occur when the trespass results in the diminution of the quality, condition, or value of the chattel. *Sotelo v. DirectRevenue, LLC*, 384 F. Supp.2d 1219, 1229 (N.D. Ill. 2005) (citing Restatement (Second) of Torts § 218(b)). The conduct need not amount to a substantial interference, but may "consist of intermeddling with or use of another's personal property." *eBay*, 100 F. Supp.2d at 1070; *see also Hamidi*, 30 Cal.4th at 1350 (noting that trespass is a remedy for "minor interferences").

Plaintiffs allege that Defendants intentionally interfered with their possessory interests in their iDevices by surreptitiously adding harmful iDevice functions and by the execution of harmful privacy-affecting code. FAC ¶¶ 118-122, 162, 167, 198, 298. Plaintiffs further contend that Defendants: accessed and obtained control over iDevices; installed code on the hard drives of the iDevices; and programmed this code to circumvent iDevice owners' privacy and security controls. FAC ¶ 302. Plaintiffs alleged that this conduct was intentional, without Plaintiffs' and Class Members' consent, or in excess of any consent given. FAC ¶¶ 173, 175, 181, 185, 189-92, 300.

Contrary to Defendants' contention that Plaintiffs have failed to identify *actionable* harm or injury, TD Br. 27, Plaintiffs specifically allege that the Defendants' conduct used memory space with a reasonable market value of $100 per 16 gigabytes. *See* FAC ¶¶ 118-122, 198; *see also eBay*, 100 F. Supp.2d at 1071 (holding that even if Defendant only used a small amount of eBay's computer system capacity, eBay was deprived of the ability to use that portion); *Sotelo*, 384 F. Supp.2d at 1230-31 (finding that Spyware interfered with and damaged computers by

*inter alia* taking up bandwidth and memory). In addition, as with *eBay*, if every ad server was permitted to put these files onto Plaintiffs' iDevices, it could potentially cause more substantive impairment of the iDevices. *eBay*, 100 F. Supp.2d at 1072; *see also, Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 438 (2nd Cir. 2004) ("By virtue of its use of a software robot, *coupled with the probability of like use by others*, Verio could interfere with Register.com's use of its own system") (emphasis added).

In addition, Plaintiffs alleged that the Defendants' actions caused a drain in batteries and shortens battery life. FAC ¶¶ 199-201. The exact quantification of the effect of Defendants' impairment of the iDevice batteries and diminution of the value of the iDevices can be discerned through discovery and expert testimony. FAC ¶ 202.

Defendants' argument that their actions were within any conceivable authority provided by Plaintiffs is disingenuous. TD Br. 27. The case cited by Defendants to support this position involved a situation where Plaintiffs' voluntarily downloaded and installed software on their iPhones. *In re Apple & ATTM Antitrust Litig.*, 2010 WL 3521965 at *7 (N.D. Cal.). In the instant action, Plaintiffs voluntarily downloaded the Apps, but that conduct could not constitute authorization for the Tracking Defendants to install and operate privacy-affecting code that was not necessary or related to the use of the App, and the existence of which was never disclosed. FAC ¶¶ 298-304; *eBay*, 100 F. Supp.2d at 1070 ("California does recognize a trespass claim where the defendant exceeds the scope of the consent."). The privacy-affecting code caused actual impairment of the battery life of the iDevice, as set forth above, and deprived the Plaintiffs of use of that portion of the memory taken up by the code. FAC ¶¶ 198-201, 118-121. Further, unlike *Hamidi*, 30 Cal.4th at 1356-1357, where the placement of a few email messages on a computer system could not be measured, the privacy-affecting code placed on the iDevices can

be quantified as set forth above. *Id.* Accordingly, Plaintiffs have satisfied the requirements for a claim of trespass to chattel.[38]

## XIV. PLAINTIFFS STATE A CLAIM FOR CONVERSION

To establish a claim of conversion, "a plaintiff must show 'ownership or right to possession of property, wrongful disposition of the property right and damages." *Kremen v. Cohen*, 337 F.3d 1024, 1029 (9th Cir. 2003) (citing *G.S. Rasmussen & Assocs., Inc. v. Kalitta Flying Serv., Inc.*, 958 F.2d 896, 906 (9th Cir. 1992)). Conversion is broadly defined in California. *Id.* at 1030. To be considered property, the owners must have established a claim to exclusivity and it must be (1) an interest capable of precise definition and (2) capable of exclusive possession or control. *Id.*

Plaintiffs alleged that unique data about them constitutes property. FAC ¶ 45(c); ¶ 72(e) and (o), ¶ 349. While this Court has noted that some courts have found that "personal information" does not constitute money or property under the UCL, other courts have found a property right in personal information under other statutes. *See Graczyk*, 660 F.3d at 277 (noting that the DPPA prohibits DMVs from disclosing personal information from motor vehicle records). Plaintiffs have alleged specific, clearly defined items that constitute property, including the UDID, zip code (*see Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal.4th 524, 534 (2011) (holding a zip code constitutes personal identification information)), App ids and passwords. FAC ¶ 64. This information should be, and is capable of being, in the control of Plaintiffs – it was contained on the Plaintiffs' iDevices, which was within their control. Plaintiffs have also sufficiently alleged that this property, contained within their iDevices, was exclusively theirs to choose what to do with in value-for-value exchanges. FAC ¶¶ 189-193.

[38] Contrary to Defendants' contention, the trespass to chattel claim does not sound in fraud. The Plaintiffs' claim goes beyond Defendants' deception in gaining access to the devices. *See U-Haul Co. of Nevada, Inc. v. U.S.*, No. 2:08-CV-729-KJD-RJJ, 2011 WL 3273873 at *3 (D. Nev. 2011) (motion to dismiss denied where Plaintiffs alleged that defendant wrongly took, possessed, and used confidential information, and the confidential information was impaired and lost its value once it was in defendant's possession).

Defendants cannot legitimately argue that Plaintiffs do not have the exclusive right to control their personal information.

## XV. PLAINTIFFS STATE AN ACTIONABLE CLAIM FOR COMMON COUNTS, *ASSUMPSIT*, AND RESTITUTION

Plaintiffs adequately allege a claim for *assumpsit*: (1) As part of their implied-at-law agreements Defendants knew, should have known, or were obligated to know that the iDevices permitted consumer data to be unknowingly released to third parties but sold the devices anyway, without disclosing the defect (FAC ¶¶ 353-54), (2) as a result thereof Defendants received money or property from Plaintiffs and Class members (money and valuable tracking data to Apple and valuable data to the Tracking Defendants) (FAC ¶¶ 353), (3) Plaintiffs and the Class Members' reasonable privacy expectations implied in such agreements were frustrated by Defendants' illegal conduct, (FAC ¶ 354), and (4) based on principles of *assumpsit* and quasi-contract under such circumstances, as between Plaintiffs and Defendants, it is unjust for Defendants to retain such monies that directly flowed from the challenged conduct (FAC ¶¶ 355-57). These allegations state a claim based on *assumpsit*, restitution and quasi-contract and thus should not be dismissed. *See Horvath v. LG Communications*, 2012 U.S. Dist. LEXIS 19215, *31-32 (S.D. Cal. Feb. 13, 2012); *McBride v. Boughton*, 123 Cal.App.4th 379, 394 (2004); and *Grewal v. Choudhury*, 2008 U.S. Dist. LEXIS 54731, at *14 (N.D. Cal. May 30, 2008). Contrary to Defendants' contention, "common count satisfies the minimum requirements of Rule 8(a)." *Sidebotham v. Robinson*, 216 F.2d 816, 827, n.4 (9th Cir. 1954). Further, despite Defendants' contention, Plaintiffs may plead *assumpsit* as an alternative legal theory. *Oracle Corp. v. SAP, AG*, No. C-07-1648, 2008 WL 5234260, at *9 (N.D.Cal. 2008).

Defendants also assert Plaintiffs do not state a viable cause of action for unjust enrichment because unjust enrichment is not an independent legal claim. The legal concept underlying such an equitable claim based on principles of *assumpsit* and restitution is that, where there is a fair and reasonable doubt whether a plaintiff can recover on a strict contract theory, but the equities require prevention of unjust enrichment, such facts give rise to a claim for relief under such a theory of recovery. *Leoni v. Delany*, 83 Cal.App.2d 303, 307-08 (1948). The Ninth

Circuit, Federal district courts, California Supreme Court and California Courts of Appeal have recognized that a claim for unjust enrichment, however denominated, may be proper, either independently or as a component of an alternate quasi-contract, *assumpsit* or restitution claim. *Paracor Fin., Inc. v. Gen. Elec. Capital Corp*., 96 F.3d 1151, 1167 (9th Cir. 1996) (under California law, "unjust enrichment is an action in quasi-contract"); *Ghirardo v. Antonioli,* 14 Cal.4th 39, 51 (1996) ("an individual may be required to make restitution if he is unjustly enriched at the expense of the other."); *McKell*, 142 Cal.App.4th at 1490 ("unjust enrichment is a basis for obtaining restitution based on quasi-contract"); *First Nationwide Savings v. Perry*, 11 Cal.App.4th 1657, 1669-70 (1992) (upholding cause of action for unjust enrichment under California law). In *Monet v. Chase Home Finance LLC*, 2010 U.S. Dist. LEXIS 59749 (N.D. Cal. June 16, 2010), Judge Seeborg provided a detailed analysis of California law on this issue. Harmonizing the cases on this issue (several of which are relied upon by Defendants in opposing this claim), he explained why, based on the appropriate circumstances, such a claim is proper, no matter what label is technically applied to it:

> In several key respects, though, the two approaches do not necessarily compete and can be harmonized. Under both views, the effect of unjust enrichment is remedied with some form of restitution. *See, e.g., Doe I v. Wal-Mart Stores, Inc.*, 572 F.3d 677, 684 (9th Cir. 2009) ("Unjust enrichment is commonly understood as a theory upon which the remedy of restitution may be granted."); Restatement of Restitution § 1 (1936) ("A person who has been unjustly enriched at the expense of another is required to make restitution to the other."). Given the appropriate facts (the independent claim concept would characterize what follows as "elements"), a plaintiff advances a basis for obtaining restitution if he or she demonstrates defendant's receipt and unjust retention of a benefit. *See Lectrodryer v. SeoulBank*, 77 Cal.App.4th 723, 726, 91 (2000); *First Nationwide Savings v. Perry*, 11 Cal.App.4th 1657, 1662-63 (1992).

*Id.* at *7-8. *See also Astiana v. Ben & Jerry's Homemade, Inc.*, 2011 U.S. Dist. LEXIS 57348, *28-30 (N.D. Cal. May 26, 2011) (analyzing case law and denying motion to dismiss where unjust enrichment claim part of claim of restitution based on quasi-contract); *Manhattan Motorcars, Inc. v.. Automobili Lamboghini,S.p.A.*, 244 F.R.D. 204, 219 (S.D.N.Y. 2007) (same); *In re Dynamic Random Access Memory (DRAM) Antitrust Litig*., 536 F.Supp.2d 1129, 1145-46

(N.D. Cal 2008) (dismissing, but upheld with clarifying amendments, an unjust enrichment claim based on violation of anti-trust laws). Accordingly, Plaintiffs are entitled to seek restitution for Defendants' conduct in unjustly enriching themselves at Plaintiffs' expense, under a common count and general *assumpsit*.

## CONCLUSION

For the foregoing reasons, Defendants' Motions to Dismiss should be denied. However, if the Court is inclined to grant Defendants' Motions to Dismiss, in whole or in part, Plaintiffs respectfully request an opportunity to replead.

Date: March 8, 2012

Respectfully submitted,
KAMBERLAW, LLC

By: s/Scott A. Kamber
Scott A. Kamber (*pro hac vice*)
KAMBERLAW, LLC
Interim Class Counsel

SCOTT A. KAMBER (*pro hac vice*)
DAVID A. STAMPLEY (*pro hac vice*)
*skamber@kamberlaw.com*
*dstampley@kamberlaw.com*
KAMBERLAW, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 202-6364

DEBORAH KRAVITZ (SBN 275661)
dkravitz@kamberlaw.com
KAMBERLAW, LLP
141 North St.
Healdsburg, California 95448
Telephone: (707) 820-4247
Facsimile: (212) 202-6364

*Interim Class Counsel*

WILLIAM AUDET
JONAS P. MANN
MICHAEL A. MCSHANE
AUDET & PARTNERS LLP

221 Main Street, Suite 1460
San Francisco, California 94105
Telephone: (415) 568-2555
Facsimile: (415) 568-2556

*Plaintiffs' Liaison Counsel*

JAY EDELSON
jedelson@edelson.com
SEAN REIS
sreis@edelson.com
EDELSON MCGUIRE, LLC
350 N LaSalle St.
Chicago IL 60654,
Telephone: (312) 589-6370

RICHARD A. LOCKRIDGE
ROBERT K. SHELQUIST
rlockridge@locklaw.com
rshelquist@locklaw.com
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue S., Suite 2200
Minneapolis, MN 55401
Telephone: (612) 339-6900
Facsimile: (612) 339-0981

JEFF S. WESTERMAN
jwesterman@milberg.com
MILBERG LLP
One California Plaza
300 South Grand Avenue, Ste 3900
Los Angeles, California 90071
Telephone: (213) 617-1200
Facsimilie: (213) 617-1975

PETER E. SEIDMAN
ANDREI V. RADO
ANNE MARIE VU (Bar No. 238771)
pseidman@milberg.com
arado@milberg.com
avu@milberg.com
MILBERG LLP
One Pennsylvania Plaza, 49th Floor
New York, New York 10119
Telephone: (212) 594-5300
Facsimile: (212) 868-1229

JEREMY WILSON

jeremy@wtlfirm.com
WILSON TROSCLAIR & LOVINS
302 N. Market Street, Suite 501
Dallas, Texas 75202
Telephone: (214) 430-1930

*Plaintiffs' Executive Committee*