DEFENDING DATA PRIVACY CLASS ACTION LITIGATION

Excerpted from Chapter 26 (Data Privacy) of
E-Commerce and Internet Law: Legal Treatise with Forms 2d Edition
A 5-volume legal treatise by Ian C. Ballon (Thomson/West Publishing, www.IanBallon.net)

PRIVACY + SECURITY FORUM
GEORGE WASHINGTON UNIVERSITY
WASHINGTON, D.C.
OCTOBER 14-16, 2019

Ian C. Ballon
Greenberg Traurig, LLP

Silicon Valley:	Los Angeles:
1900 University Avenue, 5th Fl.	1840 Century Park East, Ste. 1900
East Palo Alto, CA 914303	Los Angeles, CA 90067
Direct Dial: (650) 289-7881	Direct Dial: (310) 586-6575
Direct Fax: (650) 462-7881	Direct Fax: (310) 586-0575

Ballon@gtlaw.com
<www.ianballon.net>
LinkedIn, Twitter, Facebook: IanBallon

GT GreenbergTraurig

Ian C. Ballon

Shareholder
Internet, Intellectual Property & Technology Litigation

Admitted: California, District of Columbia and Maryland
Second, Third, Fourth, Fifth, Seventh, Ninth, Eleventh and Federal Circuits
U.S. Supreme Court
JD, LLM, CIPP/US

Ballon@gtlaw.com
LinkedIn, Twitter, Facebook: IanBallon

Silicon Valley
1900 University Avenue
5th Floor
East Palo Alto, CA 94303
T 650.289.7881
F 650.462.7881

Los Angeles
1840 Century Park East
Los Angeles, CA 90067
T 310.586.6575
F 310.586.0575

Ian Ballon is a litigator who is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property & Technology Practice and represents Internet, technology, mobile and other companies in intellectual property and internet- and mobile-related litigation, including the defense of data privacy, security breach, and TCPA class action suits. He is also the author of the leading treatise on Internet law, *E-Commerce and Internet Law: Treatise with Forms 2d edition,* the 5-volume set published by West (www.IanBallon.net). In addition, he is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009). He also serves as Executive Director of Stanford University Law School's Center for E-Commerce, which hosts the annual Best Practices Conference where lawyers, scholars and judges are regularly featured and interact. A list of recent cases may be found at http://www.gtlaw.com/Ian-C-Ballon-experience.

Mr. Ballon was named the Lawyer of the Year for Information Technology Law in the 2019, 2018, 2016 and 2013 editions of Best Lawyers in America. In both 2018 and 2019 he was recognized as one of the Top 1,000 trademark attorneys in the world for his litigation practice by *World Trademark Review*. In addition, in 2019 he was named one of the top 20 Cybersecurity lawyers in California and in 2018 one of the Top Cybersecurity/Artificial Intelligence lawyers in California by the *Los Angeles and San Francisco Daily Journal*. He received the "Trailblazer" Award, Intellectual Property, 2017 from *The National Law Journal* and he has been recognized as a "Groundbreaker" in *The Recorder*'s 2017 Litigation Departments of the Year Awards. In addition, he was the 2010 recipient of the State Bar of California IP Section's Vanguard Award for significant contributions to the development of intellectual property law (http://ipsection.calbar.ca.gov/IntellectualPropertyLaw/IPVanguardAwards.aspx). He is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also has been recognized by *The Daily Journal* as one of the Top 75 IP litigators in California in every year that the list has been published, from 2009 through 2019, and has been listed as a Northern California Super Lawyer every year from 2004 through 2018 and as one of the Top 100 lawyers in California. Mr. Ballon also holds the CIPP/US certification from the International Association of Privacy Professionals (IAPP).

26.15 Class Action Litigation

Since 2010, there has been an explosion of data privacy-related putative class action suits filed against Internet companies, social networks, social gaming sites, advertising companies, application providers, mobile device distributors, and companies that (regardless of the nature of their business) merely advertise on the Internet, among others. While data privacy class actions have been brought since the 1990s, the dramatic increase in suits filed beginning in 2010 largely results from increased attention given to data privacy in Washington during the early years of the Obama Administration, including Congressional hearings and talk of potential consumer privacy legislation, the FTC's ongoing focus on behavioral advertising, and publicity about the settlement of two high profile putative class action suits where defendants paid large sums at the very outset of each case without engaging in significant litigation. More recent disclosures about Cambridge Analytica and others have focused Congressional attention on internet and mobile businesses and their data collection practices. All of these developments, in turn, have created greater press attention and consumer awareness of privacy issues.

Businesses potentially risk being sued if they engage in practices that are at variance with their stated privacy policies or in the event of a security breach that results in the disclosure of personally identifying information where li-

ability for the breach can be established.[1]

Increasingly, however, lawsuits are brought challenging the use of new technologies or business models or for online advertising practices. Putative privacy class action suits also often are filed following FTC investigations or news reports of alleged violations or even blog reports about new product features.

Many businesses opt to settle putative class action suits—regardless of the merits—because the cost of settling often is less than the cost of litigation or to avoid adverse publicity. For a consumer-oriented company, constant press reports and blog posts about litigation alleging privacy violations may be damaging to its business. Some class action lawyers exploit this fact by issuing press releases or giving interviews or speeches designed to maximize the impact of adverse publicity and try to force a settlement. A quick settlement may resolve the problem of bad publicity, but also may identify a company as a prime target for future cases. Some businesses believe that if they are willing to fight on the merits they may be less likely targets when the next round of potential cases are filed. Ultimately, many factors influence a company's decision to either litigate or settle a case.

Earlier waves of Internet privacy litigation had largely proven unfruitful for plaintiffs' lawyers because of the absence of any monetary injury and the difficulty of framing alleged Internet privacy violations into computer crime statutes largely concerned with protecting the security of networks and systems from hackers, rather than specifically user privacy, as underscored by early litigation over the alleged collection of user information in cookie files[2] and in suits against airline companies for allegedly sharing pas-

---

[Section 26.15]

[1]Security breach class action suits are separately analyzed in section 27.07.

[2]*See, e.g., Chance v. Avenue A, Inc.*, 165 F. Supp. 2d 1153 (W.D. Wash. 2001) (granting defendants' motion for summary judgment and denying as moot plaintiffs' motion for class certification in a case arising out of defendants' alleged placement of cookies on user computers and tracking their activity; granting summary judgment on plaintiffs' claims under (1) the Computer Fraud and Abuse Act, because the minimum $5,000 damage requirement could not be met; (2) the Stored Communications Act, 18 U.S.C.A. §§ 2701 *et seq.*, because in light of the technological and commercial relationship between users and the defendant's website, it was implausible to suggest that "access" was not intended or authorized; and

senger data.[3]

---

(3) the Wiretap Act, 18 U.S.C.A. §§ 2510 *et seq.*, based on the finding that it was implicit in the code instructing users' computers to contact the website that consent had been obtained to the alleged interception of communications between users and defendants); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (granting defendant's motion to dismiss with prejudice claims arising out of DoubleClick's proposed plan to allow participating websites to exchange cookie files obtained by users to better target banner advertisements because, among other things, defendant's affiliated websites were the relevant "users" of internet access under the Electronic Communications Privacy Act (ECPA), submissions containing personal data made by users to defendant's affiliated websites were intended for those websites, and therefore the sites' authorization was sufficient to grant defendant's access under 18 U.S.C.A. § 2701(c)(2)); *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272 (C.D. Cal. 2001) (dismissing with leave to amend claims under 18 U.S.C.A. § 2511 and 18 U.S.C.A. § 1030 arising out of the alleged collection of information in cookie files because plaintiffs had failed to sufficiently allege a tortious or criminal purpose or that they had suffered damage or loss, but denying defendants' motion to dismiss plaintiffs' claim under 18 U.S.C.A. § 2701 for intentionally accessing electronically stored data); *see also, e.g., In re Pharmatrak, Inc. Privacy Litig.*, 292 F. Supp. 2d 263 (D. Mass. 2003) (granting summary judgment for the defendant on plaintiffs' ECPA claim over the alleged collection of data from cookie files, based on the lack of evidence of intent). *But see In re Toys R Us, Inc. Privacy Litig.*, No. 00-CV-2746, 2001 WL 34517252 (N.D. Cal. Oct. 9, 2001) (denying defendant's motion to dismiss plaintiffs' Computer Fraud and Abuse Act claim in a case alleging the collection of information from cookie files and granting leave for plaintiffs to amend their complaint to assert a Wiretap Act claim); *see also In re Apple & AT & TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008) (following *Toys R Us* in permitting plaintiffs to aggregate their individual damages under the CFAA to reach the $5,000 threshold).

[3]*See, e.g., In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299 (E.D.N.Y. 2005) (dismissing a suit brought on behalf of airline passengers alleging that JetBlue had transferred personal information about them to a data mining company, holding that the airline's online reservation system did not constitute an "electronic communication service" within the meaning of the Electronic Communications Privacy Act and the airline was not a "remote computing service" under the Act merely because it operated a website and computer servers); *In re American Airlines, Inc. Privacy Litig.*, 370 F. Supp. 2d 552 (N.D. Tex. 2005) (dismissing a putative class action suit brought over American's allegedly unauthorized disclosure of its passengers' personally identifiable travel information to the Transport Safety Administration and its subsequent disclosure of that information to private research companies because the alleged disclosures did not violate ECPA, plaintiffs could not state a claim for breach of contract and plaintiffs' other state law claims were preempted by the Airline Deregulation Act, 49 U.S.C.A. § 41713(b)(1)); *Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196 (D.N.D. 2004) (dismissing putative class action claims of passengers who alleged that the airline's unauthorized disclosure of their personal information to the government violated

A decade later, cases began to focus on the alleged disclosure of information through the use of social networks, behavioral advertising, mobile phone applications and other web 2.0 technologies, and cloud computing applications, although these cases often suffer from similar defects (at least under federal statutes).[4]

---

the Electronic Communications Privacy Act and constituted breach of contract where the court held that the airline was not an "electronic communications service provider" within the meaning of the Act and the airline's privacy policy did not constitute a contract).

[4]*See, e.g., In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3d Cir. 2015) (affirming dismissal of plaintiffs' federal Wiretap Act, Stored Communications Act, and Computer Fraud and Abuse Act claims and claims for violation of the California Invasion of Privacy Act (CIPA), California's Consumer Legal Remedies Act (CLRA), the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200), and the California Comprehensive Computer Data Access and Fraud Act (Cal. Penal Code § 502), but holding that plaintiffs stated claims under the California Constitution and California tort law), *cert. denied*, 137 S. Ct. 36 (2016); *In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014) (affirming in part, reversing in part dismissal of claims arising out of the alleged transmission of personal information about users from a social network to third party advertisers); *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922 (N.D. Cal. 2015) (dismissing plaintiffs' Wiretap, SCA and related claims premised on the alleged disclosure of browsing history via cookies); *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2015 WL 1503429 (N.D. Cal Apr. 1, 2015) (dismissing claims under the Stored Communications Act over alleged sharing of users' personal information with app vendors, but allowing breach of contract, breach of the implied duty of good faith and fair dealing and unfair competition claims to proceed); *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962 (N.D. Cal. 2015) (granting in part, denying in part defendants' motion to dismiss relating to the transfer of data from user's mobile address books to defendants when users selected the "Find Friends" feature to connect with friends on social networks); *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836 (N.D. Cal. 2014) (denying defendant's motion to dismiss ECPA and CIPA claims, but dismissing plaintiffs' UCL claim); *In re Google, Inc. Privacy Policy Litigation*, 58 F. Supp. 3d 968 (N.D. Cal. 2014) (dismissing with prejudice plaintiffs' CLRA and intrusion upon seclusion claims against Google for allegedly disclosing user data to third parties, but allowing claims for breach of contract and fraudulent business practices under the UCL to proceed); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018 (N.D. Cal. 2014) (dismissing all of plaintiffs' claims against all defendants with leave to amend, with the exception of the claim for common law intrusion upon seclusion; plaintiffs alleged that the defendant's apps had been surreptitiously accessing and disseminating contact information stored by customers on Apple devices); *Yunker v. Pandora Media, Inc.*, No. 11–CV–03113 JSW, 2014 WL 988833 (N.D. Cal. Mar. 10, 2014) (dismissing with prejudice plaintiff's privacy claim under the California Constitution but denying defendant's motion to dismiss plaintiff's breach of contract claim

In 2010, for example, a number of suits were brought alleging that flash cookies[5] were being used to "re-spawn" data that had been removed by users when they deleted their browser cookies, which was a practice that the defendants in these suits denied engaging in. While the first round of cases settled early on terms that provided broad releases as part of a class action settlement,[6] subsequent claims were dismissed on the merits in 2011.[7]

---

premised on Pandora's alleged breach of its privacy policy and plaintiffs' UCL claims); *Del Vecchio v. Amazon.com, Inc.*, No. C11-366-RSL, 2011 WL 6325910 (W.D. Wash. Dec. 1, 2011) (dismissing with leave to amend a putative class action suit for Computer Fraud and Abuse Act and state unfair competition, unjust enrichment and trespass claims based on the alleged use of browser and flash cookies); *In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) (dismissing for lack of Article III standing, with leave to amend, a putative class action suit against Apple and various application providers alleging misuse of personal information without consent); *Bose v. Interclick, Inc.,* No. 10 Civ. 9183, 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011) (dismissing with prejudice all claims against the advertising defendants and CFAA and most other claims against the remaining defendant in a suit alleging the use of flash cookies and browser sniffing); *LaCourt v. Specific Media, Inc.,* No. SACV 10-1256-GW (JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011) (dismissing with leave to amend a putative class action suit brought over the alleged use of flash cookies to store a user's browsing history).

[5]In contrast to browser cookies, flash cookies may be used in conjunction with flash media players to record information such as a user's volume preference, as a persistent identifier or for other purposes. *See supra* § 26.03.

[6]The first suits, brought primarily against Internet advertising companies Quantcast and Clearspring and their alleged advertiser customers, were consolidated and settled for $2.4 million and an injunction against Quantcast and Clearspring, and broad releases to all downstream advertisers and websites on which Quantcast or Clearspring widgets had been placed. *See In re Quantcast Advertising Cookie Litig.*, Case No. CV 10-5484-GW (JCGx) (C.D. Cal. Final Order and Judgment entered June 13, 2011); *In re Clearspring Flash Cookie Litig.*, Case No. CV 10-5948-GW (JCGx) (C.D. Cal. Final Order and Judgment entered June 13, 2011).

[7]*See Del Vecchio v. Amazon.com, Inc.*, No. C11-366-RSL, 2011 WL 6325910 (W.D. Wash. Dec. 1, 2011) (dismissing with leave to amend a putative class action suit for Computer Fraud and Abuse Act and state unfair competition, unjust enrichment and trespass claims based on the alleged use of browser and flash cookies); *Bose v. Interclick, Inc.,* No. 10 Civ. 9183, 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011) (dismissing with prejudice all claims against the advertising defendants and most claims against the remaining defendant in a suit alleging the use of flash cookies and browser sniffing); *LaCourt v. Specific Media, Inc.,* No. SACV 10-1256-GW (JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011) (dismissing with leave to amend a putative class action suit brought over the al-

Data privacy cases based on behavioral advertising, information voluntarily disclosed by users in social networking profiles or to app providers or other practices related to cloud computing generally involve, at most, theoretical violations where no injury has occurred.

In a typical behavioral advertising suit, for example, if the plaintiffs' assertions are correct, at most, users might have been shown an advertisement potentially of interest to the user based on the websites accessed by a computer's browser, as opposed to an advertisement for herbal Viagra substitutes, unaccredited universities or other ads of no interest to most users. In either case, the user was free to disregard the advertisement, which typically is displayed on sites that offer free content.[8] Similarly, in either case, the advertiser and ad agency generally would not know the identity of the user—only the persistent identifiers associated with a given computer (which could be used by a single person or multiple people).

Putative privacy class action suits often are filed in waves—as class action lawyers focus on new federal or state statutes, technologies, or business practices.

Plaintiffs' counsel typically try to sue under statutes that authorize prevailing parties to recover statutory damages and attorneys' fees, since actual damages typically are *de minimis* or non-existent in most of these cases. Consequently, suits often are brought in federal court under federal statutes that provide for statutory damages or attorneys' fee awards (or both), where it also may be easier for plaintiffs' class action lawyers to justify larger settlements based on

---

leged use of flash cookies to store a user's browsing history). The *Specific Media* case ultimately was dismissed by the plaintiff.

[8]Data privacy cases increasingly challenge advertising practices that in many respects are not much different from the way that television viewers are shown advertisements based on what the advertiser assumes to be the interests of the demographic group likely to be watching a particular program. Whether the advertiser is correct—and a user is interested in lip gloss rather than laxatives, for example—implicates "injuries," if any, that are at most *de minimis*. The fact that a user might have been shown an ad that he or she was free to ignore but which might have been of interest is not the sort of "violation" which typically is compensable. *See* Ian C. Ballon & Wendy Mantell, Suing Over Data Privacy and Behavioral Advertising, ABA Class Actions, Vol. 21, No. 4 (Summer 2011).

nation-wide classes.[9] Putative data privacy class action suits have been brought under the Electronic Communications Privacy Act (ECPA),[10] which in Title I (also known as the Wiretap Act) proscribes the intentional *interception* of electronic communications and in Title II (also known as the Stored Communications Act) prohibits unauthorized, intentional *access* to stored information. Plaintiffs also have sued under the Computer Fraud and Abuse Act,[11] which like ECPA, is largely an anti-hacking statute. Suits also have been brought under the Video Privacy Protection Act.[12] Claims additionally may be asserted under state law for breach of contract based on alleged breach of privacy policies and terms of use, under state computer crime statutes, for common law privacy claims or for unfair competition, where plaintiffs assert supplemental jurisdiction or jurisdiction under the Class Action Fairness Act (CAFA)[13] as the basis for federal subject matter jurisdiction. In the absence of injury or damage, however, many of these cases may not survive in federal court because injury typically is required to establish standing and is an element of many potential claims.

While standing typically is an issue in data privacy cases because plaintiffs seek to be in federal court to represent larger, national putative classes, the same considerations may not apply when claims are brought exclusively under a state statute that only may be asserted by state residents, such as the Illinois Biometric Privacy Act.[14] In such cases, plaintiff's counsel may prefer to be in state court, whereas it is the defendant who seeks to remove the case to federal court.[15]

To have standing to sue in federal court under Article III

---

[9]State courts generally certify class actions involving state residents.

[10]18 U.S.C.A. §§ 2510 to 2521 (Title I), 2701 to 2711 (Title II); *supra* § 26.09; *see generally infra* §§ 44.06, 44.07, 47.01, 50.06[4], 58.06[3].

[11]18 U.S.C.A. § 1030; *supra* § 26.09; *see generally infra* § 44.08 (analyzing the statute in greater depth).

[12]18 U.S.C.A. § 2710; *see generally supra* § 26.13[10].

[13]28 U.S.C.A. § 1332(d).

[14]740 Ill. Comp. Stat. Ann. 14/1 to 14/25.

[15]Some BIPA cases have addressed standing in this context, where the case was removed from state court by the defendant, and once in federal court the defendant moves to dismiss for lack of statutory standing (so that the case will be dismissed) but does not want to argue, based on the same facts, that the court lacks Article III jurisdiction, in which case

of the U.S. Constitution, a plaintiff must have (1) suffered

---

the suit would be remanded back to state court. The plaintiff, in turn, does not want to argue that there is Article III standing, because the plaintiff would prefer to have the case remanded to state court, and instead argues that the burden of establishing Article III standing is on the defendant when the case has been removed to federal court by the defendant. As observed by one court,

> Procedurally, Howe finds himself in an awkward position. To succeed in his lawsuit, he must establish that he is a "person aggrieved" who has statutory standing to assert a cause of action under BIPA. However, if he has a cognizable injury under BIPA, then it follows that he also has constitutional standing and must proceed in a disfavored forum. Therefore, in an effort to achieve remand without fatally undermining his claims, Howe declines to take a position on constitutional standing and argues that it is Defendants' burden to establish such standing. . . .
>
> To avoid remand, Defendants find themselves having to establish that Howe has suffered a sufficient injury for purposes of Article III standing even as their motion to dismiss vigorously contests the adequacy of his injury for purposes of statutory standing. Yet it is possible for Defendants to thread this needle. Constitutional standing and statutory standing are distinct inquiries. . . . And a plaintiff may well have Article III standing to maintain an action, but nonetheless lack statutory standing because the statute under which he or she is suing does not supply a cause of action to individuals in the plaintiff's position. *See Thompson v. N. Am. Stainless, LP*, 562 U.S. 170, 178 (2011).

Howe v. Speedway LLC, No. 17-cv-07303, 2018 WL 2445541, at *3-4 (N.D. Ill. May 31, 2018) (citations omitted) (remanding the case back to state court); *see also Goings v. UGN, Inc.,* No. 17-cv-9340, 2018 WL 2966970 (N.D. Ill. June 13, 2018) (following *Howe* in remanding plaintiff's suit alleging BIPA violations and common law negligence back to state court for lack of Article III standing, where plaintiff was aware that he was providing his biometric data to defendants and did not claim that defendants further disclosed it, and where, as in *Howe,* the defendant challenged only statutory standing to preserve its ability to stay in federal court but those arguments "cast doubt" on the basis for Article III standing); *Roberts v. Dart Container Corp.,* No. 17 C 9295, 2018 WL 3015793, at *1 (N.D. Ill. Mar. 12, 2018) (remanding to state court plaintiff's BIPA claim where the defendant had removed plaintiff's case to federal court and then promptly filed a Rule 12(b)(1) motion to dismiss for lack of standing; "To say that the current state of affairs regarding the issues at hand is a legal and logical mire would be an understatement. . . . Because the parties are in "agreement" that subject-matter jurisdiction is lacking, the Court remands the case . . . ."); *Barnes v. ARYZTA, LLC,* 288 F. Supp. 3d 834, 836-39 (N.D. Ill. 2017) (remanding plaintiff's BIPA suit to state court where the defendant failed to meet its burden of establishing Article III standing in a case it removed to federal court; "On the one hand, Plaintiff seeks remand to the state court and therefore does not want to argue to this Court it has sustained a concrete injury-in-fact because then it would be conceding subject matter jurisdiction in federal court. Defendant, on the other hand, would like to argue that Plaintiff has not sustained an Article III injury but has withdrawn any argument to that effect in a ploy to avoid being forced out of federal court. The difference between the two parties is that Plaintiff does not have to take a position on the standing is-

an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision.[16] In data privacy cases, which frequently involve alleged technical violations with no resulting economic harm, standing determinations frequently turn on whether a plaintiff has suffered an "injury in fact," which must be (a) "concrete and particularized" and (b) "actual or imminent, not conjectural or hypothetical."[17] To establish injury in fact, "allegations of possible future injury are not sufficient."[18] Where standing is based on the risk of a future injury, the threatened injury must be "certainly impending . . . ."[19]

In addition to showing injury in fact, (1) a plaintiff must

---

sue while Defendant does, because Defendant bears the burden of establishing jurisdiction in this Court.").

[16]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *citing Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180-81 (2000).

[17]*Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992). The Constitution limits the judicial power of the federal courts to actual cases and controversies. U.S. Const. art. III, § 2, cl. 1. A case or controversy exists only when the party asserting federal jurisdiction can show "such a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends." *Baker v. Carr*, 369 U.S. 186, 204 (1962). Absent Article III standing, there is no "case or controversy" and a federal court lacks subject matter jurisdiction over the suit. *Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 101 (1998); *see also Whitmore v. Arkansas*, 495 U.S. 149, 154–55 (1990) ("Article III . . . gives the federal courts jurisdiction over only 'cases and controversies.' ").

For common law claims, the only standing requirement is that imposed by Article III of the Constitution. "When a plaintiff alleges injury to rights conferred by a statute, two separate standing-related inquiries pertain: whether the plaintiff has Article III standing (constitutional standing) and whether the statute gives that plaintiff authority to sue (statutory standing)." *Katz v. Pershing, LLC*, 672 F.3d 64, 75 (1st Cir. 2012), *citing Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 89, 92 (1998). Article III standing presents a question of justiciability; if it is lacking, a federal court has no subject matter jurisdiction over the claim. *Id.* By contrast, statutory standing goes to the merits of the claim. *See Bond v. United States*, 564 U.S. 211, 218-19 (2011).

[18]*Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013) (internal quotation marks omitted).

[19]*Clapper v. Amnesty International USA*, 568 U.S. 398, 409-10 (2013); *see generally infra* § 27.07 (analyzing *Clapper* in connection with security breach putative class action suits).

establish that there is "a causal connection between the injury and the conduct complained of" (specifically, "the injury has to be fairly trace[able] to the challenged action of the defendant, and not th[e] result [of] the independent action of some third party not before the court") and (2) "it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision."[20] In short, standing depends on a showing of injury in fact, causation and redressability.[21] Where standing cannot be established, a putative class action suit will be dismissed.

Standing must be established based on the named plaintiffs that actually filed suit, not unnamed putative class members.[22]

A number data of privacy putative class action suits and claims have been dismissed for lack of standing. In many cases—particularly those involving alleged user tracking and behavioral advertising practices[23] the failure to provide

---

[20]*Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–61 (1992) (internal citations and quotations omitted); *see also Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013) ("To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.' "; *quoting Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149-50 (2010)); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180–81 (2000) (applying the same standard as *Lujan*).

[21]*Katz v. Pershing, LLC*, 672 F.3d 64, 71–72 (1st Cir. 2012) (explaining *Lujan*).

[22]*See, e.g.*, *Simon v. Eastern Ky. Welfare Rights Org.*, 426 U.S. 26, 40 n.20 (1976) ("That a suit may be a class action . . . adds nothing to the question of standing, for even named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.' "; *quoting Warth v. Seldin*, 422 U.S. 490, 502 (1975)); *see also O'Shea v. Littleton*, 414 U.S. 488, 494 (1974) ("if none of the named plaintiffs purporting to represent a class establishes the requisite of a case or controversy with the defendants, none may seek relief on behalf of himself or any other member of the class."); *Payton v. County of Kane*, 308 F.3d 673, 682 (7th Cir. 2002) ("Standing cannot be acquired through the back door of a class action." (internal quotation omitted)); *see also Easter v. American West Financial*, 381 F.3d 948, 962 (9th Cir. 2004) (holding that a court must first evaluate the standing of named plaintiffs before determining whether a class may be certified).

[23]*See, e.g.*, *Bernardino v. Barnes & Noble Booksellers, Inc.*, 17-CV-04570 (LAK) (KHP), 2017 WL 3727230, at *5-6 (S.D.N.Y. Aug. 11, 2017)

(recommending that plaintiff's motion for a preliminary injunction under the Video Privacy Protection Act be denied for lack of Article III standing); *In re Facebook Internet Tracking Litigation*, No. 5:12-md-02314-EJD, 2017 WL 2834113, at *3 (N.D. Cal. June 30, 2017) (dismissing plaintiff's claims for violations of the CDAFA, fraud, larceny, and trespass to chattels for lack of Article III standing); *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301, at *8-16 (N.D. Cal. Dec. 21, 2016) (granting summary judgment in favor of Google on plaintiff's individual claims for breach of contract, breach of the duty of good faith and fair dealing and unfair competition under California law, for lack of standing, based on evidence presented by the parties); *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 931-34 (N.D. Cal. 2015) (dismissing plaintiffs' complaint where their allegation of a secondary market for data wasn't coupled with any assertion that plaintiffs have been unable to participate in that market as a result of the defendant's alleged practices); *In re Google Android Consumer Privacy Litig.,* No. 11-MD-02264, 2013 WL 1283236, at *3-6 (N.D. Cal. Mar. 26, 2013) (rejecting diminution in the value of plaintiffs' PII, diminished battery capacity, overpayment or costs incurred as grounds to show injury-in-fact to sustain Article III standing, but holding plaintiffs had standing to assert a claim under the California Constitution and for statutory violations); *Gaos v. Google Inc.*, No. 5:10-CV-4809 EJD, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) (granting defendant's motion to dismiss claims for fraudulent misrepresentation, negligent misrepresentation, public disclosure of private facts, actual and constructive fraud, breach of contract and unjust enrichment, for lack of standing, with leave to amend, in a putative class action suit based on the defendant's alleged practice of including the search terms employed by a user in the URL for the search results page displayed in response to a search query, allegedly causing that information to be visible to advertisers in the referer header when a user clicks on an advertiser's link from the results page, but denying the motion with respect to plaintiffs' Stored Communications Act claim); *Low v. LinkedIn Corp.,* No. 11-cv-01468-LHK, 2011 WL 5509848, at *3-4 (N.D. Cal. Nov. 11, 2011) (granting defendant's motion to dismiss, for lack of standing, with leave to amend, a putative privacy class action suit based on alleged privacy violations stemming from the alleged disclosure of personally identifiable browsing history to third party advertising and marketing companies where plaintiff was unable to articulate what information of his, aside from his user identification number, had actually been transmitted to third parties, or how disclosure of his anonymous user ID could be linked to his personal identity); *Cohen v. Facebook, Inc.*, No. C 10-5282 RS, 2011 WL 5117164 (N.D. Cal. Oct. 27, 2011) (dismissing with prejudice plaintiffs' statutory right of publicity claims over the use of the names and likenesses of non-celebrity private individuals without compensation or consent in connection with Facebook's "Friend Finder" tool, for failing to allege injury sufficient to support standing, where plaintiffs could not allege that their names and likenesses had any general commercial value and did not allege that they suffered any distress, hurt feelings, or other emotional harm); *In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011) (dismissing for lack of Article III standing, with leave to amend, a putative class action suit against Apple and various application providers al-

notice[24] or other alleged privacy violations[25]—there simply has been no injury from the complained of activity.

Even in security breach cases, standing may be an issue if

---

leging misuse of personal information without consent); *Cohen v. Facebook, Inc.*, 798 F. Supp. 2d 1090 (N.D. Cal. 2011) (dismissing California common law and statutory right of publicity, California unfair competition and Lanham Act claims for lack of injury, with leave to amend, in a putative privacy class action suit based on Facebook's use of a person's name and likeness to alert their Facebook friends that they had used Facebook's "Friend Finder" tool, allegedly creating an implied endorsement); *LaCourt v. Specific Media, Inc.*, No. SACV 10-1256-GW (JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011) (dismissing a putative class action suit brought over the alleged use of flash cookies to store a user's browsing history).

[24]*See, e.g.*, *Murray v. Time Inc.*, No. C 12-00431 JSW, 2012 WL 3634387 (N.D. Cal. Aug. 24, 2012) (dismissing, with leave to amend, plaintiff's claims under Cal Civil Code § 1798.83 and Cal. Bus. & Professions Code § 17200 for lack of statutory standing due to lack injury and dismissing plaintiff's claim for injunctive relief for lack of Article III standing), *aff'd mem.*, 554 F. App'x 654 (9th Cir. 2014); *see generally supra* § 26.13[6][D] (analyzing section 1798.83 and cases construing it).

[25]*See, e.g.*, *McCollough v. Smarte Carte, Inc.*, Case No. 16 C 03777, 2016 WL 4077108, at *3-5 (N.D. Ill. Aug. 1, 2016) (dismissing plaintiff's putative Illinois Biometric Information Privacy Act class action suit for lack of Article III and statutory standing where the plaintiff alleged that Smarte Carte retained her fingerprint biometric information without written consent, where Smarte Carte used a person's fingerprints to allow them to access a rented locker, because '[e]ven without prior written consent to retain, if Smarte Carte did indeed retain the fingerprint data beyond the rental period, the Court finds it difficult to imagine, without more, how this retention could work a concrete harm" and she could not establish that she was "aggrieved by" the alleged violation, to establish statutory standing); *Frezza v. Google Inc.,* No. 5:12-cv-00237, 2013 WL 1736788 (N.D. Cal. Apr. 22, 2013) (dismissing claims for breach of contract and breach of implied contract over Google's alleged failure to implement Data Security Standards (DSS) rules in connection with promotions for Google Tags; distinguishing cases where courts found standing involving the disclosure of personal information, as opposed to mere retention of data, as in *Frezza*); *In re Google, Inc. Privacy Policy Litig.*, No. C 12-01382 PSG, 2012 WL 6738343 (N.D. Cal. Dec. 28, 2012) (dismissing claims arising out of Google's new privacy policy where plaintiffs alleged injury based on the cost of replacing their Android phones "to escape the burden imposed by Google's new policy" but in fact could not allege that they had ever purchased a replacement mobile phone and where plaintiffs could not state a claim for a violation of the Wiretap Act; relying in part on *Birdsong v. Apple, Inc.*, 590 F.3d 955, 960–61 (9th Cir. 2009) (dismissing for lack of standing a putative class action suit brought by iPod users who claimed that they suffered or imminently would suffer hearing loss because of the iPod's capacity to produce sound as loud as 120 decibels, where plaintiffs at most could claim a risk of future injury to others and therefore could not allege an injury concrete and particularized to themselves)).

there has been no allegation of injury (although there presently is a split of authority over whether the mere apprehension of future injury is sufficient to establish standing in a case where there has been a security breach but no actual identity theft or other adverse use of the information—some courts hold that it is not,[26] while others will find standing[27]).

---

[26]*See, e.g.*, *Whalen v. Michaels Stores, Inc.*, 689 F. App'x 89 (2d Cir. 2017) (affirming that the plaintiff lacked standing to sue for breach of implied contract and under N.Y. Gen. Bus. L. § 349 where she alleged that she made purchases via a credit card at a Michaels store prior to Michaels' security breach and that thereafter fraudulent charges were attempted, but she did not allege that any fraudulent charges were actually incurred by her, and she did not allege with any specificity that she spent time or money monitoring her credit); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 45 (3d Cir. 2011) (affirming dismissal for lack of standing and failure to state a claim, noting that particularly "[i]n data breach cases where no misuse is alleged, . . . there has been no injury," and that "[a]ny damages that may occur here are entirely speculative and dependent on the skill and intent of the hacker."), *cert. denied*, 566 U.S. 989 (2012); *Beck v. McDonald*, 848 F.3d 262 (4th Cir. 2017) (holding that patients at a Veterans Affairs hospital who sued alleging that their personal information had been compromised as a result of two data security breaches did not have standing because an enhanced risk of future identity theft was too speculative to cause injury in fact and the allegations were insufficient to establish a substantial risk of harm); *In re SuperValu, Inc., Customer Data Security Breach Litig.*, 870 F.3d 763 (8th Cir. 2017) (affirming dismissal of the claims of 15 of the 16 plaintiffs but holding that the one plaintiff who alleged he had suffered a fraudulent charge on his credit card had standing to sue for negligence, breach of implied contract and unjust enrichment, among other claims); *Antman v. Uber Technologies, Inc.*, Case No. 3:15-cv-01175-LB, 2018 WL 2151231 (N.D. Cal. May 10, 2018) (dismissing, with prejudice, plaintiff's claims, arising out of a security breach, for allegedly (1) failing to implement and maintain reasonable security procedures to protect Uber drivers' personal information and promptly notify affected drivers, in violation of Cal. Civ. Code §§ 1798.81, 1798.81.5, and 1798.82; (2) unfair, fraudulent, and unlawful business practices, in violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; (3) negligence; and (4) breach of implied contract, for lack of Article III standing, where plaintiff could not allege injury sufficient to establish Article III standing); *In re Science Applications International Corp. (SAIC) Backup Tape Data that Theft Litigation*, 45 F. Supp. 2d 14, (D.D.C. 2014) (granting in part and denying in part defendant's motion to dismiss plaintiffs' claims arising out of a government data breach; holding, (1) the risk of identity theft alone was insufficient to constitute "injury in fact" for purposes of standing; (2) invasion of privacy alone was insufficient to constitute "injury in fact" for purposes of standing; (3) allegations that victims lost personal and medical information was too speculative to constitute "injury in fact" for purposes of standing; (4) mere allegations that unauthorized charges were made to victims' credit cards or debit cards following theft of data failed to show causation; (5) plaintiffs' claim that victims

Where standing has been found in putative data privacy

---

received a number of unsolicited calls from telemarketers and scam artists following data breach did not suffice to show causation, as required for standing; but (6) allegations that a victim received letters in the mail from credit card companies thanking him for applying for a loan were sufficient to demonstrate causation; and (7) allegations that a victim received unsolicited telephone calls on her unlisted number from insurance companies and others targeted at her specific, undisclosed medical condition were sufficient to demonstrate causation); *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1092-95 (N.D. Cal. 2013) (dismissing plaintiffs' putative class action suit arising out of a hacker gaining access to their LinkedIn passwords and email addresses, for lack of Article III standing, where plaintiffs alleged no injury or damage); *see generally infra* § 27.07 (analyzing standing in putative data security breach class action suits).

[27]*See, e.g., Galaria v. Nationwide Mutual Insurance Co.*, 663 F. App'x 384 (6th Cir. 2016) (holding, by a 2-1 decision in an unreported opinion, that the plaintiffs had standing to sue); *Dieffenbach v. Barnes & Noble, Inc.*, 887 F.3d 826, 827-30 (7th Cir. 2018) (holding that plaintiffs had stated a claim for damages and therefore had standing to assert California and Illinois state law claims against a merchant for a security breach arising out of compromised PIN pads used to verify credit card information, where one plaintiff was injured because (1) her bank took three days to restore funds someone else had used to make a fraudulent purchase, (2) she had to spend time sorting things out with the police and her bank. and (3) she could not make purchases using her compromised account for three days; and the other plaintiff alleged that (1) her bank contacted her about a potentially fraudulent charge on her credit card statement and deactivated her card for several days, and (2) the security breach at Barnes & Noble "was a decisive factor" when she renewed a credit-monitoring service for $16.99 per month); *Lewert v. P.F. Chang's China Bistro Inc.*, 819 F.3d 963, 967-68 (7th Cir. 2016) (finding standing in a case where plaintiffs did not allege identity theft and where it appears their information may not even have been exposed, based on the present harm caused by plaintiffs having to cancel their cards); *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 695 (7th Cir. 2015) (holding that plaintiffs had standing to sue in a data breach case, where their credit card numbers had been compromised, even though they had not been victims of identity theft, where Neiman Marcus's offer of credit monitoring was construed to underscore the severity of the risk and "[p]resumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities"); *In re Zappos.com, Inc.*, 888 F.3d 1020, 1023-30 (9th Cir. 2018) (holding that plaintiffs, whose information had been stolen by a hacker but who had not been victims of identity theft or financial fraud, nevertheless had Article III standing to maintain suit in federal court, relying on the fact that other parties had alleged financial harm from the same security breach, which the court found evidenced the risk to these plaintiffs, who did not allege similar harm but alleged the threat of future harm, and because, after the breach, Zappos provided routine post-breach precautionary advice about changing passwords, which the panel considered to be an acknowledgement by Zappos that the informa-

class action suits, it has been because a plaintiff can allege entitlement to monetary damages[28] or the alleged breach of a privacy policy,[29] or, where sensitive personal data has been compromised, based on the risk of future identity theft, where this theory has been applied.[30] Less commonly, Article

---

tion taken gave the hackers the means to commit financial fraud or identity theft); *Attias v. Carefirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017) (following the Seventh Circuit's decision in *Remijas v. Neiman Marcus Group, LLC*, in holding that plaintiffs, whose information had been exposed but who were not victims of identity theft, had plausibly alleged a heightened risk of future injury to establish standing because it was plausible to infer that a party accessing plaintiffs' personal information did so with "both the intent and ability to use the data for ill."), *cert. denied*, 138 S. Ct. 981 (2018); *see generally infra* § 27.07 (analyzing standing in putative data security breach class action suits).

[28]*See, e.g.*, *Perkins v. LinkedIn Corp.*, 53 F. Supp. 2d 1190 (N.D. Cal. 2014) (holding that plaintiffs had Article III standing to bring common law right of publicity, UCL, and section 502 causes of action because an individual's name has economic value where the name is used to endorse or advertise a product to the individual's friends and contacts); *In re LinkedIn User Privacy Litigation*, Case No. 5:12–CV–03088–EJD, 2014 WL 1323713 (N.D. Cal. Mar. 28, 2014) (holding that plaintiff had sufficiently established standing under Article III and the UCL because she alleged that she purchased her premium subscription in reliance on LinkedIn's alleged misrepresentation about the security of user data); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785 (N.D. Cal. 2011) (holding that plaintiffs had standing to bring a class action suit where they alleged entitlement to compensation under California law based on Facebook's alleged practice of placing members' names, pictures and the assertion that they had "liked" certain advertisers on other members pages, which plaintiffs alleged constituted a right of publicity violation, unfair competition and unjust enrichment).

[29]*See, e.g., Carlsen v. GameStop, Inc.*, 833 F.3d 903, 908-10 (8th Cir. 2016) (finding standing in a putative data privacy class action suit where the plaintiff alleged that Game Informer Magazine shared his PII with Facebook whenever users employed Facebook's Like, Share or Comment functions on Game Informer's website, allegedly in violation of the terms of its Terms of Service, which incorporated its Privacy Policy, but affirming dismissal for failure to state a claim).

[30]*See, e.g.*, *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688, 695 (7th Cir. 2015) (security breach where some members of the putative class had already been the victims of identity theft); *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th Cir. 2010) (suit for negligence and breach of contract by employees who had had their personal information, including names, addresses, and social security numbers, compromised as a result of the theft of a company laptop); *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942 (S.D. Cal. 2014) (granting in part and denying in part defendants' motion to dismiss plaintiffs' allegations that defendants failed to provide reasonable network

III standing also may be established based on invasion of a constitutional right.[31]

Previously, standing also was found in a number of data privacy cases based merely on a plaintiff's ability to state a claim under a federal[32] or even state[33] statute that did not

---

security, including utilizing industry-standard encryption, to safeguard plaintiffs' personal and financial information stored on defendants' network; finding that plaintiffs had sufficiently established Article III standing by plausibly alleging a "credible threat" of impending harm based on the disclosure of their personal information following the intrusion); *see generally infra* § 27.07 (analyzing standing in data security putative class action cases). As noted earlier in this section, there is a significant split of authority on how courts view standing in security breach cases where information has been exposed but the only harm is apprehension of future identity theft. *See generally infra* § 27.07.

[31]*See, e.g., Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980, at *3-6 (N.D. Cal. Mar. 26, 2013) (holding that plaintiff in a putative data privacy class action suit had standing based on an unspecified violation of his constitutional rights, while rejecting theories of standing based on the alleged diminution of the value of his PII, decrease in memory space resulting from use of Pandora's app and future harm).

[32]*See, e.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012) (holding, after earlier dismissing plaintiffs' original complaint for lack of standing, that plaintiffs had standing to assert Stored Communications Act and California Constitutional Right of Privacy claims, as alleged in their amended complaint, but dismissing those claims with prejudice for failure to state a claim); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1053–55 (N.D. Cal. 2012) (holding that plaintiffs established injury in fact for purposes of Article III standing by alleging a violation of their statutory rights under the Wiretap Act); *In re Hulu Privacy Litig.,* No. C 11-03764 LB, 2012 WL 2119193, at *8 (N.D. Cal. June 11, 2012) (holding that plaintiffs "establish[ed] an injury (and standing) by alleging a violation of [the Video Privacy Protection Act]"); *Gaos v. Google Inc.*, No. 5:10-CV-4809 EJD, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) (denying defendant's motion with respect to plaintiffs' Stored Communications Act claim, finding a violation of statutory rights to be a concrete injury, while dismissing claims for fraudulent misrepresentation, negligent misrepresentation, public disclosure of private facts, actual and constructive fraud, breach of contract and unjust enrichment in a putative class action suit, for lack of standing, with leave to amend, based on the defendant's alleged practice of including the search terms employed by a user in the URL for the search results page displayed in response to a search query, allegedly causing that information to be visible to advertisers in the referer header when a user clicks on an advertiser's link from the results page); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712 (N.D. Cal. 2011) (granting in part defendant's motion to dismiss but finding Article III standing in a case where the plaintiffs alleged that a social network transferred data to advertisers without their consent because the Wiretap Act creates a private right of action for any person whose electronic communication is

require a showing of damage or injury, in light of a circuit split that ultimately was resolved by the U.S. Supreme Court in 2016,[34] but which prior to that time had made federal courts in California favored venues for data privacy cases because of the Ninth Circuit's liberal view of standing (and the perception that California law and juries tend to favor plaintiffs).[35]

"intercepted, disclosed, or intentionally used," and does not require any further injury), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim but reversing dismissal of their breach of contract and fraud claims).

[33]*See In re Google Inc. Gmail Litig.,* Case No. 13–MD–02430–LHK, 2013 WL 5423918, at *17 (N.D. Cal. Sept. 26, 2013) (denying Google's motion to dismiss plaintiffs' claim for a violation of California's anti-wiretapping and anti-eavesdropping statute, Cal. Penal Code § 630, based on Google's alleged automatic scanning of Gmail messages for keywords for the purpose of displaying relevant advertising); *see also In re Google Inc. Gmail Litigation*, Case No. 5:13-MD-2430-LHK, 2014 WL 294441 (N.D. Cal. Jan. 27, 2014) (denying the defendant's motion to certify the opinion for interlocutory appeal).

[34]*See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

[35]Prior to the U.S. Supreme Court's decision in *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016), courts in the Sixth, Eighth and Ninth Circuits found standing where a plaintiff could state a claim for violation of a statute, even where the statute did not require a showing of injury or harm and the plaintiff could not allege injury or harm apart from the alleged statutory breach, but courts in the Fourth and Federal Circuits found no standing in such cases absent a separate allegation of injury-in-fact. *See generally infra* § 27.07 (analyzing standing in the context of data security cases and discussing the circuit split that existed prior to *Spokeo*).

In *Edwards v. First American Corp.*, 610 F.3d 514 (9th Cir. 2010), *cert. dismissed*, 567 U.S. 756 (2012), the Ninth Circuit had held that a plaintiff had standing to sue a title insurer under the anti-kickback provisions of Real Estate Settlement Procedures Act, 12 U.S.C.A. § 2607, regardless of whether she was overcharged for settlement services, because the statute did not limit liability to instances in which a plaintiff was overcharged. Another Ninth Circuit panel (without citing Edwards) subsequently held that a plaintiff had standing, at least for purposes of a motion to dismiss at the outset of the case, to allege Title I and Title II ECPA claims for Wiretap and Stored Communications Act violations, among others, based on the defendants' alleged telephone surveillance, even though the court acknowledged that the plaintiff ultimately might be unable to prove that she in fact had been subject to illegal surveillance, at which point the court, on a more developed record, might conclude that plaintiff lacked standing. *See Jewel v. National Security Agency*, 673 F.3d 902, 908–911 (9th Cir. 2011); *see also Robins v. Spokeo, Inc.*, 742 F.3d 409, 412-14 (9th Cir. 2014) (holding, in a case in which the plaintiff alleged that the defendant's website published inaccurate information about him, that because the plaintiff had stated a claim for a willful violation of the

Fair Credit Reporting Act, for which actual harm need not be shown, the plaintiff had established Article III standing, where injury was premised on the alleged violation of plaintiff's statutory rights), *vacated and remanded*, 136 S. Ct. 1540 (2016); *In re Google, Inc. Privacy Policy Litigation*, Case No. C-12-01382-PSG, 2013 WL 6248499 (N.D. Cal. Dec 3, 2013) (following *Edwards* in holding that plaintiffs had established Article III injury under the Wiretap Act and the Stored Communications Act by alleging unauthorized access and wrongful disclosure of communications, including disclosure to third parties, in addition to the interception of communications); *Gaos v. Google Inc.*, No. 5:10-CV-4809 EJD, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012) (following *Edwards* in denying defendant's motion with respect to plaintiffs' Stored Communications Act claim).

Courts in the Ninth Circuit had construed *Edwards* and *Jewel* as requiring that even where a plaintiff stated a claim under a federal statute that did not require a showing of damage, plaintiffs had to allege facts to "show that the claimed statutory injury is particularized as to them." *Mendoza v. Microsoft, Inc.*, No. C14-316-MJP, 2014 WL 4540213 (W.D. Wash. Sept. 11, 2014) (dismissing plaintiffs' claims under the Video Privacy Protection Act, California Customer Records Act, California Unfair Competition Law and Texas Deceptive Trade Practices Act where plaintiffs failed to identify an injury that was actual or imminent and particularized and merely offered "broad conclusory statements and formulaic recitations" of the statutes but did not allege facts to support the allegation that Microsoft allegedly retained and disclosed personally identifiable information); *see also Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1021 (N.D. Cal. 2012) (following *Edwards* and *Jewel* in finding standing in a case alleging that LinkedIn browsing histories and user identification numbers, sent in connection with third party cookie identification numbers, were transmitted to third parties by LinkedIn, while conceding that "the allegations that third parties can *potentially* associate LinkedIn identification numbers with information obtained from cookies and can de-anonymize a user's identity and browser history are speculative and relatively weak"; emphasis in original).

The Sixth and Eighth Circuits took a similar approach. *See Beaudry v. TeleCheck Services, Inc.*, 579 F.3d 702, 707 (6th Cir. 2009) (finding "no Article III (or prudential) standing problem arises . . ." where a plaintiff can allege all of the elements of a Fair Credit Reporting Act statutory claim); *Hammer v. Sam's East, Inc.*, 754 F.3d 492, 498-500 (8th Cir. 2014) (holding that plaintiffs established Article III standing by alleging facts sufficient to state a claim under the Fair and Accurate Credit Transactions Act and therefore did not separately need to show actual damage).

The Fourth and Federal Circuits, however, rejected the proposition that alleging an injury-in-law by merely stating a claim and establishing statutory standing to sue satisfied the separate standing requirements of Article III of the U.S. Constitution. *See David v. Alphin*, 704 F.3d 327, 333, 338-39 (4th Cir. 2013) (holding that statutory standing alone is insufficient to confer Article III standing; affirming dismissal of an ERISA claim where the plaintiffs stated a claim but could not establish injury-in-fact); *Consumer Watchdog v. Wisconsin Alumni Research Foundation*, 753

In *Spokeo, Inc. v. Robins*,[36] the U.S. Supreme Court resolved this circuit split, holding that merely alleging a "statutory violation" is *not* sufficient because "Article III standing requires a concrete injury even in the context of a statutory violation."[37] *Spokeo* addressed standing under a federal statute as well as when an intangible harm may satisfy the injury in fact prong of the test for Article III standing. To establish standing, a plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision.[38]

In addressing when an intangible harm may satisfy the injury in fact requirement, Justice Alito, writing for himself and five other justices,[39] reiterated that a plaintiff must show (or at the pleading stage, simply allege[40]) that he or she has suffered " 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.' "[41]

For an injury to be *particularized,* it "must affect the

F.3d 1258, 1262 (Fed. Cir. 2014) (holding that a consumer group lacked standing to challenge an administrative ruling, explaining that " 'Congress may enact statutes creating legal rights, the invasion of which creates standing, even though no injury would exist without the statute.' *Linda R.S. v. Richard D.*, 410 U.S. 614, 617 n.3 (1973) (citations omitted). That principle, however, does not simply override the requirement of injury in fact.").

This Circuit split was resolved by *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

[36]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016).

[37]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[38]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *citing Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180-81 (2000).

[39]Justice Thomas concurred in the decision, drawing a distinction between private and public rights. Justices Ginsburg and Sotomayor dissented, arguing that the plaintiff established standing in this case.

[40]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016), *quoting Warth v. Seldin,* 422 U.S. 490, 518 (1975).

[41]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 (1992). Justice Alito explained that while Article III standing is determined by a three part test, *Spokeo* turned largely on the first factor. To establish standing, a plaintiff must have (1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable decision. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016),

plaintiff in a personal and individual way."[42] Justice Alito explained that "[p]articularization is necessary to establish injury in fact, but it is not sufficient. An injury in fact must also be 'concrete.' "[43]

To be concrete, an injury must be " 'real' and not 'abstract.' "[44] It need not be *tangible,* however. "[I]ntangible injuries can . . . be concrete."[45]

The Court identified two potential sources of authority for finding injury in fact in a case involving intangible harm. Justice Alito wrote that, in determining whether an intangible harm constitutes injury in fact, "both history and the judgment of Congress play important roles."[46] With respect to history, "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[47] Congress's "judgment is also instructive and important. . . . Congress may 'elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.' "[48] Thus, for all state and federal statutory and common law privacy claims, an intangible harm may establish standing *if* it has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts. This second consideration—the judgment of Congress—would not be applicable to common law or even state statutory remedies.[49] It could only serve as a basis for standing in a case involving a federal question claim.

---

citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992); *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.,* 528 U.S. 167, 180-81 (2000).

[42]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 560 n.1 (1992).

[43]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016).

[44]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), *citing* Webster's Third New Int'l Dictionary 472 (1971); Random House Dictionary of the English Language 305 (1967).

[45]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[46]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[47]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[48]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 578 (1992).

[49]One district court held that a state legislature could create rights sufficient to confer Article III standing "[i]n the absence of governing U.S. Supreme Court precedent . . . . " *Matera v. Google, Inc.*, Case No. 15-CV-

While the Court made clear that merely alleging a "statutory violation" is not sufficient, Justice Alito also explained that "Congress has the power to define injuries and articulate chains of causation that will give rise to a case or controversy where none existed before."[50] However, "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[51] For example, "a bare procedural violation, divorced from any concrete harm . . ." would not satisfy the injury-in-fact requirement.[52] On the other hand, "the risk of real harm" can satisfy the requirement of concreteness and, in some circumstances, even "the violation of a procedural right granted by statute can be sufficient . . . ."[53]

In remanding the case for further consideration, Justice Alito reiterated that the plaintiff in that case could not satisfy the demands of Article III by alleging a bare procedural violation of the Fair Credit Reporting Act. Similarly, Justice Alito offered that if the defendant had maintained an incorrect zip code for the plaintiff, "[i]t is difficult to imagine how the dissemination of an incorrect zip code, without more, could work any concrete harm."[54]

Spokeo was a compromise 6-2 opinion that likely would

04062-LHK, 2016 WL 5339806, at *14 (N.D. Cal. Sept. 23, 2016) (denying defendant's motion to dismiss plaintiff's California Invasion of Privacy Act claim for lack of standing). This analysis, however, is plainly wrong given that Justice Alito expressly identified the role of *Congress*, not state legislatures, in elevating claims. Moreover, state legislatures have no legal authority to confer subject matter jurisdiction over state claims on federal courts. *See, e.g., Hollingsworth v. Perry*, 133 S. Ct. 2652, 2667 (2013) ("[S]tanding in federal court is a question of federal law, not state law. And no matter its reasons, the fact that a State thinks a private party should have standing to seek relief for a generalized grievance cannot override our settled law to the contrary."); *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735 (W.D.N.Y. 2017) (citing *Spokeo* and *Hollingsworth* in finding no standing to sue under various state statutes).

[50]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), *quoting Lujan v. Defenders of Wildlife,* 504 U.S. 555, 580 (1992).

[51]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[52]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016), *citing Summers v. Earth Island Institute,* 555 U.S. 488, 496 (2009).

[53]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1549 (2016).

[54]*Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1550 (2016). On remand, the

have been decided differently had conservative Justice Scalia, who participated in oral argument for the case, not passed away before the opinion issued.[55] It is likely that his replacement on the Court, Justice Gorsuch, views standing in much the same way as the late Justice Scalia. It therefore remains to be seen whether *Spokeo* is respected as binding precedent or scaled back over time.

Spokeo is relevant to data privacy cases premised on intangible harm and violations of federal statutes. The result of *Spokeo* is that merely stating a claim under a federal statute will not be sufficient to establish standing, nor will mere procedural violations of a statute.[56] In a number of cases

---

Ninth Circuit concluded that Robins had standing under the Supreme Court's test. *See Robins v. Spokeo, Inc.*, 867 F.3d 1108 (9th Cir. 2017).

[55]*See generally infra* § 27.07 (discussing the opinion and its origins in greater detail in the context of security breach case law).

[56]*See, e.g.*, *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12, 15-17 (2d Cir. 2017) (holding that players of Take-Two's NBA 2K15 video game, which scanned players' faces, did not have Article III standing to sue for alleged violations of the Illinois Biometric Information Privacy Act, which was intended to protect against potential misuse of biometric data, because plaintiffs' alleged failure to comply with provisions regulating the storage and dissemination of biometric information and requiring notice and consent to the collection of biometric information amounted to merely "procedural violations" under *Spokeo*, where no reasonable player would have concluded that the MyPlayer feature was conducting anything other than a face scan where plaintiffs had to place their faces within 6-12 inches of the camera, slowly turn their heads to the left and right, and continue to do this for approximately 15 minutes, belying any claim of lack of consent; plaintiffs could not allege any material risk of misuse of biometric data for failing to provide notice of the duration for which the data would be held; and plaintiffs failed to show a risk of real harm from the alleged unencrypted transmission of their face scans); *Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 910-12 (7th Cir. 2017) (holding that the plaintiff lacked standing to sue for Time Warner's alleged retention of his personally identifiable information in violation of the Cable Communications Policy Act, 47 U.S.C. § 551(e), because he did not allege that "any of the personal information that he supplied to the company . . . . had been leaked or caused financial or other injury to him or had even been at risk of being leaked."; Although the Act created a right of privacy, and "[v]iolations of rights of privacy are actionable," because plaintiff did not allege that "Time Warner had released, or allowed anyone to disseminate, any of the plaintiff's personal information in the company's possession," the statutory violation alone could not confer standing); *Braitberg v. Charter Communications, Inc.,* 836 F.3d 925, 929-31 (8th Cir. 2016) (dismissing for lack of standing, as a case involving a mere procedural violation under *Spokeo,* plaintiff's putative class action suit alleging that his former cable television provider retained his personally

brought under the Fair and Accurate Credit Transactions Act (FACTA)[57] and other federal[58] or state[59] privacy statutes,

---

identifiable information in violation of the Cable Communications Policy Act because "Braitberg alleges only that Charter violated a duty to destroy personally identifiable information by retaining certain information longer than the company should have kept it. He does not allege that Charter has disclosed the information to a third party, that any outside party has accessed the data, or that Charter has used the information in any way during the disputed period. He identifies no material risk of harm from the retention; a speculative or hypothetical risk is insufficient. Although there is a common law tradition of lawsuits for invasion of privacy, the retention of information lawfully obtained, without further disclosure, traditionally has not provided the basis for a lawsuit in American courts."); *Hancock v. Urban Outfitters, Inc.,* 830 F.3d 511 (D.C. Cir. 2016) (affirming dismissal of plaintiff's claim under the D.C.'s Use of Consumer Identification Information Act, D.C. Code §§ 47–3151 *et seq*., which provides that "no person shall, as a condition of accepting a credit card as payment for a sale of goods or services, request or record the address or telephone number of a credit card holder on the credit card transaction form, . . ." for lack of standing, because "[t]he Supreme Court's decision in *Spokeo* . . . closes the door on Hancock and White's claim that the Stores' mere request for a zip code, standing alone, amounted to an Article III injury.").

[57]5 U.S.C. § 1681c(g)). FACTA seeks to reduce the risk of identity theft by, among other things, prohibiting merchants from including more than the last five digits of a customer's credit card number on a printed receipt. *See* 15 U.S.C. § 1681c(g)(1); *see generally supra* § 26.12[8]. Courts have found standing to be lacking in FACTA cases involving bare procedural violations. *See, e.g., Katz v. Donna Karan, LLC,* 872 F. 3d 114 (2d Cir. 2017) (affirming dismissal for lack of standing plaintiff's FACTA claim alleging that he twice purchased items at the defendants' stores, and on both occasions received a printed receipt that identified not only the last four digits of his credit card number but also the first six digits, because plaintiff could not meet his affirmative burden to establish subject matter jurisdiction by a preponderance of the evidence); *Crupar–Weinmann v. Paris Baguette America, Inc*., 861 F.3d 76, 81 (2d Cir. 2017) (affirming the lower court's holding that a procedural violation of FACTA—the printing of the plaintiff's credit card expiration date on her receipt—presented no material risk of harm to the underlying interest Congress sought to protect (identity theft), because Congress itself had clarified that printing the expiration date, without more, did not "increase. . . the risk of material harm of identity theft."); *Meyers v. Nicolet Restaurant of De Pere, LLC,* 843 F.3d 724, 726-29 (7th Cir. 2016) (holding that plaintiff lacked standing to sue for a FACTA violation alleging that the defendant failed to provide him with a receipt that truncated the expiration date of his credit card because "without a showing of injury apart from the statutory violation, the failure to truncate a credit card's expiration date is insufficient to confer Article III standing."); *Bassett v. ABM Parking Services, Inc.*, 883 F.3d 776, 779-83 (9th Cir. 2018) (holding that receiving "an overly revealing credit card receipt—unseen by others and unused by identity thieves

the alleged privacy violation was deemed merely a "bare

. . ." constituted a procedural violation of the FCRA that was insufficient to establish Article III standing; "We need not answer whether a tree falling in the forest makes a sound when no one is there to hear it. But when this receipt fell into Bassett's hands in a parking garage and no identity thief was there to snatch it, it did not make an injury."); *see also Daniel v. National Park Service*, 891 F.3d 762, 766-68 (9th Cir. 2018) (distinguishing *Bassett* in finding that the plaintiff had alleged a concrete, particularized injury based on identity theft and fraudulent charges that occurred after she received a debit card receipt at Yellowstone National Park that displayed the expiration date of her credit card, but holding that Article III standing was lacking because she had not alleged an injury "fairly traceable" to the violation because her actual debit card number was partially obscured and there were no facts to suggest that the exposure of the expiration date resulted in the identity theft or fraudulent charges).

[58]*See, e.g., Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 910-12 (7th Cir. 2017) (holding that the plaintiff lacked standing to sue for Time Warner's alleged retention of his personally identifiable information in violation of the Cable Communications Policy Act, 47 U.S.C. § 551(e), because he did not allege that "any of the personal information that he supplied to the company . . . . had been leaked or caused financial or other injury to him or had even been at risk of being leaked." Although the Act created a right of privacy, and "[v]iolations of rights of privacy are actionable," because plaintiff did not allege that "Time Warner had released, or allowed anyone to disseminate, any of the plaintiff's personal information in the company's possession," the statutory violation alone could not confer standing); *Braitberg v. Charter Communications, Inc.,* 836 F.3d 925, 929-31 (8th Cir. 2016) (dismissing for lack of standing, as a case involving a mere procedural violation under *Spokeo,* plaintiff's putative class action suit alleging that his former cable television provider retained his personally identifiable information in violation of the Cable Communications Policy Act because "Braitberg alleges only that Charter violated a duty to destroy personally identifiable information by retaining certain information longer than the company should have kept it. He does not allege that Charter has disclosed the information to a third party, that any outside party has accessed the data, or that Charter has used the information in any way during the disputed period. He identifies no material risk of harm from the retention; a speculative or hypothetical risk is insufficient. Although there is a common law tradition of lawsuits for invasion of privacy, the retention of information lawfully obtained, without further disclosure, traditionally has not provided the basis for a lawsuit in American courts."); *Hancock v. Urban Outfitters, Inc.,* 830 F.3d 511, 514 (D.C. Cir. 2016) (affirming dismissal of plaintiff's claim under the D.C.'s Use of Consumer Identification Information Act, D.C. Code §§ 47–3151 *et seq*., which provides that "no person shall, as a condition of accepting a credit card as payment for a sale of goods or services, request or record the address or telephone number of a credit card holder on the credit card transaction form, . . ." for lack of standing, because "[t]he Supreme Court's decision in *Spokeo* . . . . closes the door on Hancock and White's claim that the Stores' mere request for a zip code, standing alone, amounted to an Article III injury.").

procedural" violation (and therefore insufficient to establish injury in fact under *Spokeo*). Data privacy cases, of course, have been dismissed for lack of standing on other grounds[60] as well.

On the other hand, *Spokeo*'s directive to look to either

---

[59]*See, e.g.*, *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12, 15-17 (2d Cir. 2017) (holding that players of Take-Two's NBA 2K15 video game, which scanned players' faces, did not have Article III standing to sue for alleged violations of the Illinois Biometric Information Privacy Act, which was intended to protect against potential misuse of biometric data, because plaintiffs' alleged failure to comply with provisions regulating the storage and dissemination of biometric information and requiring notice and consent to the collection of biometric information amounted to merely "procedural violations" under *Spokeo*, where no reasonable player would have concluded that the MyPlayer feature was conducting anything other than a face scan where plaintiffs had to place their faces within 6-12 inches of the camera, slowly turn their heads to the left and right, and continue to do this for approximately 15 minutes, belying any claim of lack of consent; plaintiffs could not allege any material risk of misuse of biometric data for failing to provide notice of the duration for which the data would be held; and plaintiffs failed to show a risk of real harm from the alleged unencrypted transmission of their face scans), *aff'g*, *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 510-21 (S.D.N.Y. 2017).

[60]*See, e.g., Hutton v. National Board of Examiners in Optometry, Inc.*, 243 F. Supp. 3d 609, 613-15 (D. Md. 2017) (dismissing plaintiffs' claims under the California Customer Records Act, Cal. Civ. Code §§ 1798.81 *et seq*. and California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, and for breach of contract, breach of implied contract, negligence and unjust enrichment, for lack of standing, where plaintiffs alleged that, as a result of a breach of a database containing PII from optometrists throughout the United States, they had incurred time and expenses (and, for one plaintiff, received a credit card that had not been requested, issued in the name she had used when she provided her PII to the defendant), because their assumption that the defendant suffered a data breach and was the source of the leaked data was based on online conversations, where plaintiffs "failed to allege a plausible, inferential link between the provision of PII to NBEO at some point in the past and their recent receipt of unsolicited credit cards."); *McCollough v. Smarte Carte, Inc.,* Case No. 16 C 03777, 2016 WL 4077108, at *3-5 (N.D. Ill. Aug. 1, 2016) (dismissing plaintiff's putative Illinois Biometric Information Privacy Act class action suit for lack of Article III and statutory standing where the plaintiff alleged that Smarte Carte retained her fingerprint biometric information without written consent, where Smarte Carte used a person's fingerprints to allow them to access a rented locker, because '[e]ven without prior written consent to retain, if Smarte Carte did indeed retain the fingerprint data beyond the rental period, the Court finds it difficult to imagine, without more, how this retention could work a concrete harm" and she could not establish that she was "aggrieved by" the alleged violation, to establish statutory standing).

Congress or whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts has been construed in some cases to provide a basis for standing because of the nature of privacy rights at common law[61] and/or because of federal statutory claims deemed by some courts to be analogous to common law invasion of privacy, including suits brought under the Video Privacy Protection Act[62] and a Fair Credit Reporting Act claim

---

[61]*See, e.g., Mount v. PulsePoint, Inc.,* 684 F. App'x 32, 34 (2d Cir. 2017) (affirming the lower court ruling that the plaintiffs had adequately alleged standing to assert state law claims for deceptive business practices under N.Y. Gen. Bus. Law § 349 and unjust enrichment, based on loss of privacy, because PulsePoint's allegedly unauthorized accessing and monitoring of plaintiffs' web-browsing activity implicated "harms similar to those associated with the common law tort of intrusion upon seclusion so as to satisfy the requirement of concreteness."); *Boelter v. Advance Magazine Publishers Inc.,* 210 F. Supp. 3d 579 (S.D.N.Y. 2016) (denying defendant's motion to dismiss a putative class action suit brought by a subscriber to *Bon Appétit* and *Self* magazines alleging that Condé Nast disclosed her subscription information in violation of the Michigan Preservation of Personal Privacy Act, Mich. Comp. Laws §§ 445.1711 *et seq*., for lack of standing and failure to state a claim).

[62]*See, e.g., In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 272-74 (3d Cir. 2016) (holding, without much analysis, that plaintiffs had Article III standing to pursue Stored Communications Act, Video Privacy Protection Act, California Invasion of Privacy Act, New Jersey computer crime and common law privacy claims), *cert. denied,* 137 S. Ct. 624 (2017); *Van Patten v. Vertical Fitness Group, LLC,* 847 F.3d 1037, 1042-43 (9th Cir. 2017) (holding that the plaintiff had alleged sufficient harm to establish Article III standing in a TCPA case because (1) "[a]ctions to remedy defendants' invasions of privacy, intrusion upon seclusion, and nuisance have long been heard by American courts, and the right of privacy is recognized by most states" and (2) Congress, in enacting the statute, established "the substantive right to be free from certain types of phone calls and text messages absent consumer consent."); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 982-84 (9th Cir. 2017) (affirming dismissal on the merits, but first holding that the plaintiff had standing to sue for the alleged disclosure of personally identifiable information under the Video Privacy Protection Act, which the Ninth Circuit panel deemed an alleged violation of "a substantive provision that protects concrete interest."); *Perry v. CNN,* 854 F.3d 1336, 1339-41 (11th Cir. 2017) (holding that a user of the CNN mobile app had standing to sue under the Video Privacy Protection Act, where he alleged no injury other than the statutory violation, because (1) "[t]he structure and purpose of the VPPA supports the conclusion that it provides actionable rights" in prohibiting the wrongful disclosure of personal information, and (2) a VPPA claim has a close relationship to a common law right of privacy, which is a harm that has traditionally been regarded as providing a basis for a lawsuit in English

premised on a security breach.[63]

Spokeo's impact on putative security breach and TCPA class action suits is addressed in sections 27.07 and 29.16, respectively.

While many privacy cases involve merely intangible harm, injury in fact in security breach and other cases alternatively may be based on the threat of future harm. The case most directly relevant to future harm is *Clapper v. Amnesty International USA*,[64] in which the Court made clear that "allegations of possible future injury are not sufficient."[65] To justify standing based on future harm, the threatened injury must be "certainly impending" to constitute injury in fact.[66]

Even where a plaintiff can establish Article III standing, claims based on alleged data privacy violations may not fit well into existing federal statutes and may be dismissed or

---

or American courts, where "[t]he intrusion itself makes the defendant subject to liability, even though there is no publication or other use . . . . "; citing Restatement of Torts § 652B cmt. B); *In re Vizio, Inc. Consumer Privacy Litig.,* 238 F. Supp. 3d 1204, 1215-17 (C.D. Cal. 2017) (holding that plaintiffs had standing to sue under the VPPA and Wiretap Act in a putative database privacy class action suit involving data allegedly collected by a smart television manufacturer and others, based on the close relationship of these claims to common law invasion of privacy and because of Congress's judgment in enacting the VPPA); *Yershov v. Gannett Satellite Information Network, Inc.*, 204 F. Supp. 3d 353, 358-64 (D. Mass. 2016) (denying defendant's motion to dismiss for lack of Article III standing); *see generally supra* § 26.13[10] (analyzing the VPPA in greater detail).

[63]*See In re Horizon Healthcare Services Inc. Data Breach Litig.,* 846 F.3d 625, 629, 638–40 (3d Cir. 2017) (holding that plaintiffs had standing to sue for the disclosure of personal information, in violation of FCRA, as a result of the theft of two laptops, because of the statutory violation, and that the same facts would not necessarily "give rise to a cause of action under common law"; while also holding that "the 'intangible harm' that FCRA seeks to remedy 'has a close relationship to a harm [i.e., invasion of privacy] that has traditionally been regarded as providing a basis for a lawsuit in English or American courts,' *Spokeo*, 136 S. Ct. at 1549, . . . [and therefore] Congress properly defined an injury that 'give[s] rise to a case or controversy where none existed before.' "); *see generally supra* § 26.12[3] (addressing FCRA in greater detail).

[64]*Clapper v. Amnesty International USA*, 568 U.S. 398 (2013).

[65]*Clapper v. Amnesty International USA*, 568 U.S. 398, 409 (2013).

[66]*Clapper v. Amnesty International USA*, 568 U.S. 398, 409-10, 414-17 (2013); *see infra* § 27.07 (analyzing the circuit split over what level of apprehension of future injury is sufficient to establish standing in a security breach case where the plaintiffs have not experienced identity theft or other financial injury).

subject to summary judgment.

A number of data privacy suits have been brought under the Electronic Privacy Communications Act (ECPA).

ECPA authorizes claims under Title I for the intentional *interception* or disclosure of an intercepted communication, whereas claims under Title II may be based on unauthorized intentional *access* to stored communications or the intentional disclosure of those communications.[67]

In behavioral advertising and other alleged data tracking cases, it is important to understand the underlying technology to determine whether a given communication is even covered by ECPA and, if so, permitted or prohibited.

To the extent claims are based on *disclosure* under either Title I or II, as opposed to interception (under Title I) or access (under Title II), civil claims may only be based on the *contents* of a communication. Personal data such as a person's name, email address, home address, phone number or other details that could identify a person, however, are treated as non-content data, not the *contents* of a communication, which is defined under ECPA as "information concerning the substance, purport, or meaning of that communication."[68] On this basis alone, most claims premised on disclosure will not be actionable under either Title I or

---

[67] *See infra* §§ 44.06, 44.07.

[68] 18 U.S.C. § 2510(8); *see also id.* § 2703(c)(1)(A) ("a provider of electronic communication service or remote computing service may disclose a record or other information pertaining to a subscriber to or customer of such service . . . to any person other than a governmental entity."). "[I]nformation concerning the identity of the author of the communication," which is generally what is at issue in data privacy cases, is not considered "contents." *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998). As the legislative history makes clear, ECPA "exclude[s] from the definition of the term 'contents,' the identity of the parties or the existence of the communication. It thus distinguishes between the substance, purport or meaning of the communication and the existence of the communication or transactional records about it." S. Rep. No. 541, 99th Cong., 2d Sess. (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567; *see also In re Zynga Privacy Litig.*, 750 F.3d 1098, 1105-09 (9th Cir. 2014) (holding that URLs, including referer header information, did not constitute the contents of a communication under ECPA; explaining that "Congress intended the word 'contents' to mean a person's intended message to another (i.e., the 'essential part' of the communication, the 'meaning conveyed,' and the 'thing one intends to convey.')" and that "[t]here is no language in ECPA equating 'contents' with personally identifiable information."); *U.S. v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009) (holding that Call Data Content (CDC) is neither the contents of a

Title II[69] (subject to narrow exceptions, such as where a URL, which generally is considered non-content data, reveals the substance of a communication[70]).

---

communication nor a communication under Title I of ECPA; "CDC . . . is data that is incidental to the use of a communication device and contains no 'content' or information that the parties intended to communicate. It is data collected by the telephone company about the source, destination, duration, and time of a call."), *cert. denied*, 559 U.S. 987 (2010); *Viacom Int'l Inc. v. YouTube Inc.*, 253 F.R.D. 256, 265 (S.D.N.Y. 2008) (holding, in a copyright infringement suit, that YouTube was prevented by the Stored Communications Act from disclosing the content of videos marked by users as private, but ordering "production of specified non-content data about such videos" because "the ECPA does not bar disclosure of non-content data about the private videos (e.g., the number of times each video has been viewed on YouTube.com or made accessible on a third-party website through an 'embedded' link to the video)."); *see generally infra* § 50.06[4] (analyzing contents and non-contents under ECPA in greater detail and discussing additional cases).

[69]*See, e.g.*, *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 935-36 (N.D. Cal. 2015) (dismissing plaintiffs' Wiretap Act claim because the data allegedly transmitted through cookies about the browsing history of logged-out users was not the contents of a communication); *Svenson v. Google Inc.*, No. 13–cv–04080–BLF, 2015 WL 1503429, at *7-8 (N.D. Cal. Apr. 1, 2015) (applying *Zynga* in dismissing without leave to amend plaintiff's SCA claim premised on the alleged disclosure of credit card information (but not numbers), purchase authorization data, addresses, zip codes, names, phone numbers, and email addresses, in connection with the use of Google Wallet); *In re: Carrier IQ, Inc. Consumer Litig.*, 78 F. Supp. 3d 1051, 1083-84 (N.D. Cal. 2015) (dismissing Wiretap Act claim for alleged interception of user names or passwords by the Carrier IQ Software in a putative consumer class action suit); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012) (dismissing plaintiff's claim because geolocation data was not the contents of a communication and holding that "personally identifiable information that is automatically generated by the communication but that does not comprise the substance, purport, or meaning of that communication is not covered by the Wiretap Act."); *see generally infra* § 50.06[4][B].

[70]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 135-39 (3d Cir. 2015) (holding that a URL potentially could constitute the contents of a communication, depending on the context), *cert. denied*, 137 S. Ct. 36 (2016); *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1108-09 (9th Cir. 2014) (stating in *dicta* that queried URLs could incorporate the content of a communication if they reproduced words from a search engine query, but holding that the referer headers at issue in that case constituted non-content data); *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 265 (N.D. Cal. 2016) (holding that URLs shared on Facebook constituted contents); *see generally infra* § 50.06[4][B].

In one behavioral advertising case, *Yunker v. Pandora Media, Inc.*, No. 11-CV-03113 JSW, 2013 WL 1282980, at *6-7 (N.D. Cal. Mar. 26, 2013), the court held that the plaintiff stated a claim where it alleged that

For similar reasons, cases based on non-content data also may fail to state claims under California's constitutional right to privacy or California's Invasion of Privacy Act, Cal. Penal Code § 631(a).[71]

ECPA, which is comprised of the Wiretap Act (Title I) and the Stored Communications Act (Title II) was never intended to regulate data privacy generally, and certainly not in ways

---

non-content data such as a person's UUID, zip code, gender or birthday, was the actual contents of a communication to the plaintiff and not data from a non-content record. *Id.* at *6-7 (distinguishing *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012)). Merely alleging that non-content data was the substance of a communication, however, does not make it so. *See generally infra* § 50.06[4].

[71]*See, e.g.*, *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 843 (N.D. Cal. 2017) (dismissing plaintiff's CIPA claims under sections 631 and 632 because Facebook did not intercept data or eavesdrop); *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 937 (N.D. Cal. 2015) (dismissing plaintiff's CIPA claim where he did not plead facts to show how Facebook used a "machine, instrument or contrivance" to obtain the contents of communications and did not adequately allege that Facebook acquired the contents of a communication); *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1037-42 (N.D. Cal. 2014) (dismissing with leave to amend plaintiff's claim for a violation of California's constitutional right to privacy where plaintiffs alleged that Yahoo's alleged scanning, storage and disclosure of email content violated their right to privacy).

There is also some authority for the proposition that a claim under section 631 is preempted because Congress sought to occupy the field in enacting ECPA. *See Bunnell v. Motion Picture Ass'n of America*, 567 F. Supp. 2d 1148, 1154–55 (C.D. Cal. 2007) (field preemption); *see also LaCourt v. Specific Media, Inc.*, No. SACV 10-1256-GW (JCGx), 2011 WL 1661532, at *7 (C.D. Cal. Apr. 28, 2011) (characterizing a section 631 claim as "arguably" preempted under *Bunnell*). *But see Leong v. Carrier IQ, Inc.*, CV 12-01562 GAF (MRWx), 2012 WL 1463313 (C.D. Cal. Apr. 27, 2012) ("In the Court's view, the cases finding complete preemption are not persuasive."); *Valentine v. Nebuad, Inc.*, 804 F. Supp. 2d 1022 (N.D. Cal. 2011) (disagreeing that section 631 is preempted by ECPA), *citing People v. Conklin*, 12 Cal. 3d 259, 272, 114 Cal. Rptr. 241 (Cal. 1974); *Kearney v. Salomon Smith Barney*, 39 Cal. 4th 95, 106, 45 Cal. Rptr. 3d 730 (Cal. 2006); *see generally infra* § 44.09 (analyzing this issue).

States "are precluded from regulating conduct in a field that Congress, acting within its proper authority, has determined must be regulated by its exclusive governance." *Arizona v. United States,* 567 U.S. 387, 399 (2012). Preemption may be express, as it is in some statutes, or "[t]he intent to displace state law altogether can be inferred from a framework of regulation 'so pervasive . . . . that Congress left no room for the States to supplement it' or where there is a 'federal interest . . . . so dominant that the federal system will be assumed to preclude enforcement of state laws on the same subject.' " *Id., quoting Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947).

that could never have been conceived of at the time the laws were first enacted. As a statute largely intended to prohibit hacking (in Title II) or eavesdropping or interception (in Title I), ECPA is drawn narrowly in terms of what is covered, what is proscribed and what is permitted with authorization or consent.

Data privacy and behavioral advertising claims premised on unauthorized *interception*[72] under Title I have failed where there has been consent or no interception[73] (or, at

---

[72]*Intercept* means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device." 18 U.S.C. § 2510(4). To establish that a defendant "intercepted" an electronic communication, a plaintiff must allege facts that show the electronic communication has been "acquired during transmission, not while it is in electronic storage." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 878–79 (9th Cir. 2002).

[73]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 274-76 (3d Cir. 2016) (affirming dismissal of plaintiffs' Wiretap claim, holding that "Google was either a party to all communications with the plaintiffs' computers or was permitted to communicate with the plaintiffs' computers by Viacom, who was itself a party to all such communications."), *cert. denied,* 137 S. Ct. 624 (2017); *Cooper v. Slice Technologies, Inc.*, 17-CV-7102 (JPO), 2018 WL 2727888 (S.D.N.Y. June 6, 2018) (dismissing with prejudice plaintiffs' claims under the Wiretap Act, Stored Communications Act, and Cal. Penal Code § 631(a) where plaintiffs consented to the alleged disclosure of anonymized data, as set forth in the terms of the defendant's Privacy Policy); *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 844 (N.D. Cal. 2017) (dismissing plaintiff's Wiretap and CIPA claims because defendant Facebook was "a party to the communication" in one transaction and did not intercept data in either exchange); *In re Vizio, Inc. Consumer Privacy Litig.,* 238 F. Supp. 3d 1204, 1226-28 (C.D. Cal. 2017) (dismissing plaintiffs' Wiretap Act and companion California Invasion of Privacy Act claims with leave to amend where plaintiffs had "not articulated with sufficient clarity when Vizio supposedly intercepted their communications."); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1022-31 (N.D. Cal. 2014) (holding, in a putative Stored Communications Act class action suit, that the plaintiffs consented to email scanning); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1063 (N.D. Cal. 2014) (dismissing plaintiffs' Wiretap Act claim based on Path's mobile app's alleged copying and transmission of electronic address books; "Although Path allegedly transmitted the Class Members' Contact Address Books from the Class Members' mobile devices to Path's servers, Path did not 'intercept' a 'communication' to do so."); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *7–8 (N.D. Cal. Mar. 26, 2013) (holding, in a behavioral advertising case, that the plaintiff failed to state a Wiretap Act claim in part where (1) he alleged that he provided his personal information directly to Pandora and that Pandora "intercepted" the information from him, rather than alleging that the defendant used a device to intercept a communication from the plaintiff to a third party,

and (2) the communication was directed to Pandora, within the meaning of 18 U.S.C.A. § 2511(3)(A)); *Hernandez v. Path, Inc.*, No. 12-cv-01515-YGR, 2012 WL 5194120, at *3 (N.D. Cal. Oct. 19, 2012) (dismissing plaintiff's claim on the same grounds as in *Opperman*, cited above); *Marsh v. Zazoom Solutions, LLC,* No. C–11–05226–YGR, 2012 WL 952226, at * 17 (N.D. Cal. Mar. 20, 2012) (dismissing plaintiff's Wiretap Act claim in a case involving payday loans, where the plaintiff did not allege that any defendant "acquired the information by capturing the transmission of information that was otherwise in the process of being communicated to another party," or that any defendant used a "device" to intercept the communication); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712–13 (N.D. Cal. 2011) (dismissing plaintiffs' Title I claim where the communication either was directed from the user to the defendant (in which case the service was the addressee or intended recipient and therefore could disclose the communication to advertisers as long as it had its own lawful consent) or was sent from the user to an advertiser (in which case the advertiser was the addressee or intended recipient), but in either case was not actionable), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim and reversing dismissal of their breach of contract and fraud claims; plaintiffs did not appeal the dismissal of their ECPA claims); *Crowley v. Cybersource*, 166 F. Supp. 2d 1263, 1268-69 (N.D. Cal. 2001) (dismissing an interception claim premised on Amazon.com's alleged disclosure to co-defendant, Cybersource, where the plaintiff's email was sent directly to Amazon.com and was not acquired through use of a device).

In *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017), the Third Circuit expressly rejected the plaintiffs' argument that "the one-party consent language in the Wiretap Act does not apply . . . because the plaintiffs were minors who were incapable of consenting at all." *Id.* at 275. The court noted that plaintiffs could not find "any authority for the proposition that the Wiretap Act's one-party consent regime depends on the age of the non-consenting party." *Id.* The court also observed that "adopting the plaintiffs' view could mean that the alleged inability of a minor to consent would vitiate another party's consent, which we conclude would be inconsistent with the Wiretap Act's statutory language." *Id.* n.75. It further rejected plaintiffs' argument on policy grounds, "[g]iven the vast potential for unexpected liability whenever a minor happened to browse an Internet site that deployed cookies . . . ." *Id.* at 275.

In *In re Facebook Internet Tracking Litigation*, 263 F. Supp. 3d 836, 844 (N.D. Cal. 2017), Judge DaVila underscored why the Wiretap Act is often ill suited to tracking claims:

> Plaintiffs argue that Facebook's acquisition of URL data constitutes an "interception" of Plaintiffs' communications with websites they visit. . . . But Plaintiffs' argument misstates the means by which Facebook receives that data. As Facebook points out, two separate communications occur when someone visits a page where a Facebook "like" button is embedded. . . . First, the user's browser sends a GET request to the server where the page is hosted. Second, as the page loads, the code snippet for the Facebook button triggers a second, independent GET request to Facebook's servers. That second request contains the URL of the page where the "like" button is embedded, as well as

least, no interception by the defendant).[74] Collecting user data such as a customer's requested URL, the referer URL[75] (the last URL visited before a request was made) and an encrypted advertising network cookie, to provide to a third party to analyze and send targeted advertising similarly has been held to not constitute an interception where the information was collected in the ordinary course of business.[76]

The Stored Communications Act, which is Title II of ECPA, prohibits both unauthorized access (or exceeding authorized access) in section 2701,[77] subject to exceptions for access by

---

the contents of cookies that Facebook has previously set on that user's computer. The parties to the first transaction are the web user (e.g., one of the Plaintiffs) and the server where the page is located (e.g., the server that handles requests for http://www.cnn.com/). The parties to the second transaction are that same web user and a Facebook server—but not cnn.com. As to the second transaction, Facebook has not "intercepted" the communication within the meaning of the Wiretap Act because it is "a party to the communication" under 18 U.S.C. § 2511(2)(d). Facebook is not a party to the first communication (between the user and cnn.com), and it does not intercept any data that those parties exchange. The fact that a user's web browser automatically sends the same information to both parties does not establish that one party intercepted the user's communication with the other.

Id. at *4.

[74]*See, e.g.*, *Kirch v. Embarq Management Co.,* No. 10-2047-JAR, 2011 WL 3651359, at *7-9 (D. Kan. Aug. 19, 2011) (granting summary judgment for the defendant on plaintiff's claim in a putative class action suit where the court found that a third party, rather the defendant, intercepted the plaintiff's communications), *aff'd*, 702 F.3d 1245, 1246–47 (10th Cir. 2012) (holding that section 2520 does not impose civil liability on aiders or abettors), *cert. denied*, 569 U.S. 1013 (2013).

[75]*Referer* is the proper terminology, reflecting a spelling error when the term first came into common use, but courts sometimes use the term *referrer* URL or *referrer* header, rather than referer URL or referer header.

[76]*See Kirch v. Embarq Management Co.*, 702 F.3d 1245, 1248-51 (10th Cir. 2012) (holding that there was no interception, and hence no violation of ECPA, because the contents of the communications were acquired by Embarq in the ordinary course of its business within the meaning of 18 U.S.C.A. § 2510(5)(a)(ii)), *cert. denied*, 569 U.S. 1013 (2013). *But see In re Google Inc. Gmail Litig.,* Case No. 13–MD–02430–LHK, 2013 WL 5423918, at *8–12 (N.D. Cal. Sept. 26, 2013) (denying Google's motion to dismiss plaintiffs' complaint based on the argument that automatically scanning Gmail messages for keywords for purposes of displaying relevant advertising came within the exception created by section 2510(5)(a)(ii)); *see generally infra* § 44.06[1] (discussing these cases in greater detail).

[77]18 U.S.C.A. § 2701(a). Authorization may be given for a limited purpose. In *Anzaldua v. Northeast Ambulance & Fire Protection Dist.*, 793 F.3d 822, 838 (8th Cir. 2015), for example, the Eighth Circuit stated in *dicta* that where a defendant gave his ex-girlfriend his Gmail user name and password so that she could send his resume to a prospective employer,

the person or entity providing a wire or electronic communications service[78] and by a user of that service with respect to a communication of or intended for that user;[79] and knowingly divulging the contents of a communication while in electronic storage in section 2702,[80] subject to exceptions including to an addressee or intended recipient of such communication,[81] where authorized[82] and with lawful consent.[83] Behavioral advertising claims often do not fit well into this framework because they often involve communications that are either not proscribed by the Stored Communications Act or are permitted.

Section 2702 of the Stored Communications Act directs that an entity providing an electronic communication service to the public "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service."[84] However, a provider of an electronic communication service may divulge the contents of a communication to an addressee or intended recipient of such communication.[85] A provider of an electronic communication service may also access the contents of a communication with the "lawful consent" of an addressee or intended recipient of such communication.[86]

Because section 7201 addresses a knowing disclosure, it may not provide the basis for a claim based on a security breach, where the defendant-company typically is a victim that did not know about the incursion.[87]

---

and only for that purpose, subsequent access to the account would be deemed unauthorized under the SCA.

[78]18 U.S.C.A. § 2701(c)(1).

[79]18 U.S.C.A. § 2701(c)(2).

[80]18 U.S.C.A. § 2702(a).

[81]18 U.S.C.A. § 2702(b)(1).

[82]18 U.S.C.A. § 2702(b)(2).

[83]18 U.S.C.A. § 2702(b)(3).

[84]18 U.S.C.A. § 2702(a)(1).

[85]18 U.S.C.A. § 2702(b)(1).

[86]18 U.S.C.A. § 2702(b)(3).

[87]*See In re Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *42 (N.D. Cal. Aug. 30, 2017) (dismissing plaintiffs' SCA claim because plaintiffs could not plausibly allege a knowing disclosure on the part of defendants).

In *In re Facebook Privacy Litigation*,[88] the court dismissed plaintiffs' Title II claim alleging that by clicking on a banner advertisement, users unknowingly were transmitting information to advertisers, because the communication at issue either was sent to Facebook or to third party advertisers. As explained by the court:

> Under either interpretation, Plaintiffs fail to state a claim under the Stored Communications Act. If the communications were sent to Defendant, then Defendant was their "addressee or intended recipient," and thus was permitted to divulge the communications to advertisers so long as it had its own "lawful consent" to do so. 18 U.S.C. § 2702(b)(3). In the alternative, if the communications were sent to advertisers, then the advertisers were their addressees or intended recipients, and Defendant was permitted to divulge the communications to them. *Id.* § 2702(b)(1).[89]

Plaintiffs' Title I claim against Facebook likewise suffered from a similar defect in that case. The court ruled that a Wiretap Act claim may not be maintained where an allegedly unauthorized interception was either permitted by the statute or not made by the electronic communication service itself.[90]

In *Low v. LinkedIn Corp.*,[91] the court similarly dismissed with prejudice plaintiffs' Stored Communications Act claim under section 2702 based on the allegation that LinkedIn transmitted to third party advertisers and marketers the LinkedIn user ID and the URL of the LinkedIn profile page viewed by a user at the time the user clicked on an advertise-

---

[88]*In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705 (N.D. Cal. 2011), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim and reversing dismissal of their breach of contract and fraud claims; plaintiffs did not appeal the dismissal of their ECPA claims).

[89]*In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 713–14 (N.D. Cal. 2011) (footnote omitted), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014).

[90]*See In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 712–13 (N.D. Cal. 2011) (dismissing plaintiffs' Title I claim where the communication either was directed from the user to the defendant (in which case the service was the addressee or intended recipient and therefore could disclose the communication to advertisers as long as it had its own lawful consent) or was sent from the user to an advertiser (in which case the advertiser was the addressee or intended recipient), but in either case was not actionable), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014).

[91]*Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012).

ment because, even if true, LinkedIn would have been acting as neither an electronic communication service (ECS), such as a provider of email, nor a remote computing service (RCS), which provides computer storage or processing services to the public (analogous to a virtual filing cabinet used by members of the public for offsite storage).[92] In so holding, the court explained that LinkedIn IDs were numbers generated by LinkedIn, not user data sent by users for offsite storage and processing. URL addresses of viewed pages similarly were not sent to LinkedIn by plaintiffs for storage or processing.[93]

Claims under section 2701 of the Stored Communications Act, for unauthorized access (or exceeding authorized access), may fail because they only apply to material in *electronic storage* when accessed from *a facility through which an electronic communication service is provided,* which may not apply to data stored and accessed from mobile devices, tablets or personal computers.

Section 2701 requires a showing that a defendant accessed without authorization "a facility through which an electronic communication service is provided."[94] "While the computer systems of an email provider, a bulletin board system, or an ISP are uncontroversial examples of facilities that provide electronic communications services to multiple users, . . ."[95] courts have held that an individual's computer, laptop or mobile device does not meet the statutory definition of a "facility through which an electronic communication service is

---

[92]The legal regime governing ECS and RCS providers under ECPA is analyzed extensively in section 50.06[4] (service provider obligations in response to third party subpoenas and government search and seizure orders) and also touched on in sections 44.06 and 44.07 (criminal remedies).

[93]*See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1021-22 (N.D. Cal. 2012).

[94]18 U.S.C.A. § 2701(a)(1). A *facility,* according to the Eleventh Circuit, includes "the physical means or equipment for doing something." *Brown Jordan Int'l, Inc. v. Carmicle,* 846 F.3d 1167, 1177 n.4 (11th Cir. 2017) (quoting Oxford English Dictionary Online). As explained by the Third Circuit, " 'facility' is a term of art denoting where network service providers store private communications." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 147 (3d Cir. 2015), *cert. denied,* 137 S. Ct. 36 (2016); *see generally infra* § 44.08[1] (analyzing *facility* in greater detail).

[95]*In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057 (N.D. Cal. 2012).

provided" within the meaning of the Stored Communications Act.[96]

Similarly, claims premised on information stored on user devices will be difficult to maintain because the data at issue may not deemed to be in *electronic storage*. In addition to showing that a defendant intentionally accessed a facility through which an electronic communication service is provided without authorization (or exceeded authorized access), to state a claim under the Stored Communications Act a plaintiff also must show that the defendant, through this unauthorized access, "thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage . . . ."[97] *Electronic storage* is defined as "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[98] Where the information accessed is stored on a user's device (or in a cookie file[99] or a browser's toolbar and browsing history,[100] or on a

---

[96]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 146-48 (3d Cir. 2015) (holding that a user's web browser could not constitute a facility), *cert. denied,* 137 S. Ct. 36 (2016); *In re Facebook Internet Tracking Litigation*, 263 F. Supp. 3d 836, 845 (N.D. Cal. 2017) (dismissing plaintiff's amended SCA claim because, among other things, personal computers are not "facilities" under the SCA); *Cousineau v. Microsoft Corp.*, 6 F. Supp. 3d 1167, 1174-75 (W.D. Wash. 2014) (holding that a mobile device is not a facility through which an electronic communications services is provided; explaining that "[t]he fact that the phone not only received but also sent data does not change this result, because nearly all mobile phones transmit data to service providers"); *Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 755-56 (N.D. Ohio 2013) (holding that a blackberry mobile device was not a "facility" within the meaning of section 2701(a)(1) in a case brought over an employer's access to a former employee's personal Gmail account; "the g-mail [sic] server, not the blackberry, was the 'facility."); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057–58 (N.D. Cal. 2012) (operating system for computer, laptop or mobile device); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270–71 (N.D. Cal. 2001) (a user's computer); *see generally infra* § 44.07.

[97]18 U.S.C.A. § 2701(a).

[98]18 U.S.C.A. § 2510(17).

[99]*See, e.g.*, *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 936 (N.D. Cal. 2015) (dismissing plaintiffs' SCA claim because "Plaintiff's theory . . . —that Facebook accesses personal information through persistent cookies permanently residing in users' personal web

universally unique device identifier (UUID)[101] used in connection with advertising or email stored on a user's own computer[102] or a Blackberry mobile device[103]), the information is not in *electronic storage*[104] as defined in the Act.[105]

---

browsers—cannot be reconciled with the temporary nature of storage contemplated by the statutory definition."); *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 988 F. Supp. 2d 434, 447 (D. Del. 2013) (explaining, in connection with dismissing plaintiff's SCA claim, that "[t]here seems to be a consensus that '[t]he cookies' long-term residence on plaintiffs' hard drives places them outside of § 2510(17)'s definition of 'electronic storage' and, hence, [the SCA's] protection"), *aff'd in relevant part on other grounds*, 806 F.3d 125, 146-48 (3d Cir. 2015) (affirming dismissal of plaintiffs' SCA claim because a user's web browser could not constitute a facility), *cert. denied*, 137 S. Ct. 36 (2016); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512–13 (S.D.N.Y. 2001); *In re Toys R Us, Inc. Privacy Litig.,* No. 00-CV-2746, 2001 WL 34517252, at *4 (N.D. Cal. Oct. 9, 2001).

[100]*See In re Facebook Internet Tracking Litigation*, 263 F. Supp. 3d 836, 845 (N.D. Cal. 2017) (dismissing plaintiff's amended SCA claim because, among other things, the tool bar and browser history are "stored locally on the user's personal computer for the user's convenience.").

[101]*See Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 *JSW*, 2013 WL 1282980, at *8–9 (N.D. Cal. Mar. 26, 2013).

[102]*See, e.g.*, *Cohen v. Casper Sleep Inc.*, Nos. 17cv9325, 17cv9389, 17cv9391, 2018 WL 3392877, at *5 (S.D.N.Y. July 12, 2018) (dismissing plaintiff's claim against NaviStone, a marketing company and data broker that offered code to e-commerce vendors to help them identify who visited their websites by scanning visitors' computers for information that could be used for de-anonymization, because "communications stored on personal devices are not held in electronic storage."); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1057–58 (N.D. Cal. 2012) (operating system for computer, laptop or mobile device); *Hilderman v. Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1204–05 (S.D. Cal. 2008).

[103]*See Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013) (denying defendants' motion to dismiss but holding that the plaintiff could not prevail to the extent that she sought to recover "based on a claim that Kulmatycki violated the SCA when he accessed e-mails which she had opened but not deleted. Such e-mails were not in 'backup' status as § 2510(17)(B) uses that term or 'electronic storage' as § 2701(a) uses that term.").

[104]Under the statute, 'electronic storage' means (1) 'any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,' or (2) 'any storage of such communication by an electronic communication service for purposes of backup protection of such communication.' " *Anzaldua v. Northeast Ambulance & Fire Protection Dist.*, 793 F.3d 822, 839 (8th Cir. 2015), *quoting* 18 U.S.C.A. § 2510(17). In *Anzaldua*, the court held that a draft email was not in *electronic storage*; "because the email had not been sent, its storage on the Gmail server was not 'temporary, intermediate,' and 'incidental to the

As explained by one court, "[t]itle II deals only with facilities operated by electronic communications services such as 'electronic bulletin boards' and 'computer mail facilit[ies],' and the risk that communications temporarily stored in these facilities could be accessed by hackers."[106] In other words, email stored on Gmail, Hotmail or Yahoo! servers or private messages stored on Facebook or MySpace servers are different from cookie files or other content stored locally on the hard drive of a user's home or office computer, laptop, tablet or mobile phone.

Even where a *prima facie* claim may be stated, section 2701 creates an express exclusion for conduct authorized "by a user of that service with respect to a communication of or intended for that user."[107] ECPA defines a *user* as "any person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use."[108] Accordingly, courts have held that App providers and websites that accessed personal information from mobile phones or website cookies were *users* within the meaning of ECPA (and any disclosure of personal information therefore was authorized and not actionable).[109] For purposes of ECPA, consumers or other *end users* are not the

---

electronic transmission thereof.' " 793 F.3d at 840, *quoting* 18 U.S.C.A. § 2510(17). Likewise, the sent version of the same email was not stored for backup purposes; Gmail stores sent messages as a matter of course, not as a duplicate backup. 793 F.3d at 840-42 (noting disagreement among various courts about what constitutes backup). As the Eighth Circuit explained, the SCA "is not a catch-all statute designated to protect the privacy of stored Internet communications; instead, it is narrowly tailored to provide a set of Fourth-Amendment-like protections for computer networks." *Anzaldua v. Northeast Ambulance & Fire Protection Dist.*, 793 F.3d 822, 839 (8th Cir. 2015), *quoting* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004).

[105] *See generally supra* § 44.07 (analyzing the issue in greater detail).

[106] *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 512–13 (S.D.N.Y. 2001) (cookie files stored on a user's computer).

[107] 18 U.S.C.A. § 2701(c)(2).

[108] 18 U.S.C.A. § 2510(13).

[109] *See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 274-76 (3d Cir. 2016) (affirming dismissal of plaintiffs' Wiretap claim, holding that "Google was either a party to all communications with the plaintiffs' computers or was permitted to communicate with the plaintiffs' computers by Viacom, who was itself a party to all such communications."), *cert. denied*, 137 S. Ct. 624 (2017); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1060 (N.D. Cal. 2012) (holding that "because the com-

users referenced by the statute.[110] In the nomenclature of the statute, end users, or consumers, are referred to as *customer* or *subscribers*.[111]

Pursuant to section 2511(2)(d), a website operator also may be deemed an intended recipient of communications, such as data included in website cookies[112] or otherwise on a

---

munications [personal information stored on user iPhones, accessed by App providers when users downloaded and installed Apps on their phones] were directed at the App providers, the App providers were authorized to disclose the contents of those communications to the Mobile Industry Defendants."); *In re Zynga Privacy Litig.,* No. C 10-04680 JWW, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011) (dismissing plaintiffs' Wiretap and Stored Communications Act claims under Titles I and II of ECPA, with leave to amend, where "the electronic communications in question were sent to Defendant itself, to Facebook, or to advertisers, but both Acts exempt addressees or intended recipients of electronic communications from liability for disclosing those communications."); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 508–09 (S.D.N.Y. 2001) (holding that DoubleClick-affiliated websites are *users* under the statute and therefore authorized to disclose any data sent to them).

[110]*In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 509 (S.D.N.Y. 2001) (noting that the definition of *user* refers to a person or entity). In *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012), the court held that certain mobile advertising providers, but not Apple itself, were authorized recipients of personal information pursuant to section 2701(c). The court explained:

> Plaintiffs allege that Apple itself caused a log of geolocation data to be generated and stored, and that Apple designed the iPhone to collect and send this data to Apple's servers . . . . Apple, however, is neither an electronic communications service provider, nor is it a party to the electronic communication between a user's iPhone and a cellular tower or WiFi tower. Thus, the Court fails to see how Apple can avail itself of the statutory exception by creating its own, secondary communication with the iPhone. With respect to the Mobile Industry Defendants, Plaintiffs allege that when users download and install Apps on their iPhones, the Mobile Industry Defendants' software accesses personal information on those devices and sends that information to Defendants . . . . Thus, the App providers are akin to the web sites deemed to be "users" in *In re DoubleClick*, and the communications at issue were sent to the App providers. *See* 154 F. Supp. 2d at 508–09. Thus, because the communications were directed at the App providers, the App providers were authorized to disclose the contents of those communications to the Mobile Industry Defendants. The Mobile Industry Defendants' actions therefore fall within the statutory exception of the SCA.

In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1060 (N.D. Cal. 2012).

[111]*See infra* § 50.06[4] (analyzing permitted and prohibited disclosures under ECPA in greater detail).

[112]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 140-45 (3d Cir. 2015) (affirming dismissal of plaintiffs' Wiretap Act claim where plaintiffs alleged that "defendants acquired the

user's hard drive.[113]

In addition, mistaken disclosures are not actionable under the Stored Communications Act. In *Long v. Insight Communications of Central Ohio, LLC*,[114] the defendant had mistakenly provided the wrong subscriber information in response to a subpoena in a child pornography investigation. The Bureau of Criminal Investigation traced several hundred files containing child pornography to a particular IP address. Investigators requested a grand jury subpoena requiring Time Warner Cable to provide subscriber information linked to the IP address. TWC complied, but mistakenly disclosed subscriber information tied to a different IP address. The person wrongly misidentified and his family sued under the SCA (and for state law claims). In dismissing plaintiffs' putative class action suit, the Sixth Circuit held that the requirements that SCA violations be undertaken *knowingly* and *intentionally* were not met when the defendant did not realize that it was providing the wrong subscriber information in response to the subpoena. The Sixth Circuit held that to impose liability under section 2707(a), there must be "a showing that the provider knew not only that it was divulging information (i.e., that the act of disclosure was not inadvertent), but also what information was being divulged (i.e., the facts that made the disclosure unauthorized)."[115]

Further, even when a Stored Communications Act claim

---

plaintiffs' internet history information when, in the course of requesting webpage advertising content at the direction of the visited website, the plaintiffs' browsers sent that information directly to the defendants' servers. Because the defendants were the intended recipients of the transmissions at issue—i.e. GET requests that the plaintiffs' browsers sent directly to the defendants' servers— . . . § 2511(2)(d) means the defendants have done nothing unlawful under the Wiretap Act."), *cert. denied*, 137 S. Ct. 36 (2016).

[113]*See, e.g.*, *Cohen v. Casper Sleep Inc.*, Nos. 17cv9325, 17cv9389, 17cv9391, 2018 WL 3392877, at *3 (S.D.N.Y. July 12, 2018) (dismissing plaintiff's claim against NaviStone, a marketing company and data broker that offered code to e-commerce vendors to help them identify who visited their websites by scanning visitors' computers for information that could be used for de-anonymization, because "§ 2511 is a one-party consent statute. . . . It is clear that the retailers were parties to the communications and NaviStone had their consent. . . . [And] ISPs are intermediaries who facilitate electronic communications, not recipients of such communications.").

[114]*Long v. Insight Communications of Central Ohio, LLC*, 804 F.3d 791 (6th Cir. 2015).

[115]*Long v. Insight Communications of Central Ohio, LLC*, 804 F.3d

can be stated, at least two circuits have held that a plaintiff may not recover statutory damages under the SCA unless he or she has incurred actual damages.[116]

In addition to user authorization, both Title I and Title II of ECPA create express exceptions where consent has been obtained from customers or subscribers.[117] Customer or subscriber consent may be obtained through assent to the provisions of a Privacy Policy or Terms of Use and thereby provide a defense in litigation. As noted in the House Report,

> a subscriber who places a communication on a computer 'electronic bulletin board,' with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the communication. If conditions governing disclosure or use are spelled out in the rules of an electronic communication service, and those rules are available to users or in contracts for the provision of such services, it would be appropriate to imply consent on the part of a user to disclosures or uses consistent with those rules.[118]

Courts have entered judgment for the defendant or dismissed putative privacy class action suits where consent was inferred from TOU or a Privacy Policy.[119]

In contrast to Title II, Title I addresses communications in

791, 797 (6th Cir. 2015). The Sixth Circuit also affirmed the district court's rulings that, on the same facts, the defendant did not commit intentional disclosure of private information under Ohio law, intentional infliction of emotional distress or breach of contract.

[116]*See Van Alstyne v. Electronic Scriptorium, Ltd.*, 560 F.3d 199, 208 (4th Cir. 2009); *Vista Mktg., LLC v. Burkett*, 812 F.3d 954, 965 (11th Cir. 2016).

[117]*See* 18 U.S.C.A. §§ 2511(2)(d), 2511(3)(b)(ii), 2702(b)(3).

[118]H.R. Rep. No. 99-647, 99th Cong., 2d Sess. 66 (1986).

[119]*See, e.g.*, *Williams v. Affinion Group, LLC*, 889 F.3d 116, 120-23 (2d Cir. 2018) (affirming summary judgment for defendants on the ECPA claims of former participants in an online membership program, in a putative class action suit, finding consent under section 2511(2)(d) based on their acceptance of website Terms & Conditions); *Cooper v. Slice Technologies, Inc.*, 17-CV-7102 (JPO), 2018 WL 2727888 (S.D.N.Y. June 6, 2018) (dismissing with prejudice plaintiffs' claims under the Wiretap Act, Stored Communications Act, and Cal. Penal Code § 631(a) where plaintiffs consented to the alleged disclosure of anonymized data, as set forth in the terms of the defendant's Privacy Policy); *Cain v. Redbox Automated Retail, LLC*, 136 F. Supp. 3d 824 (E.D. Mich. 2015) (granting summary judgment in favor of Redbox on plaintiffs' Michigan Video Rental Privacy Act, breach of contract and unjust enrichment claims in a putative class action suit where the plaintiffs provided written permission to Redbox to allow it to disclose information as set forth in its Privacy Policy); *Garcia v. Enterprise*

Holdings, Inc., 78 F. Supp. 3d 1125, 1135-37 (N.D. Cal. 2015) (dismissing plaintiff's California Invasion of Privacy Act claim with leave to amend where the defendant—app provider's Terms of Use and Privacy Policy provided consent for the alleged disclosures); *In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1027-31 (N.D. Cal. 2014) (granting defendant's motion to dismiss with prejudice plaintiffs' Wiretap Act claim based on the allegation that Yahoo scanned and analyzed emails to provide personal product features and targeted advertising, detect spam and abuse, create user profiles, and share information with third parties, and stored email messages for future use based on explicit consent set forth in the Yahoo Global Communications Additional Terms of Service for Yahoo Mail and Yahoo Messenger agreement); *Perkins v. LinkedIn Corp.*, 53 F. Supp. 2d 1190 (N.D. Cal. 2014) (dismissing Wiretap Act and SCA claims because plaintiffs consented to LinkedIn's collection of email addresses from users' contact lists through LinkedIn's disclosure statements); *Del Vecchio v. Amazon.com, Inc.*, No. C11-366-RSL, 2011 WL 6325910 (W.D. Wash. Dec. 1, 2011) (dismissing, with leave to amend, a trespass and CFAA claim based on the alleged use of browser and flash cookies where, among other things, the potential use of browser and flash cookies was disclosed to users in the defendant's "Conditions of Use and Privacy Notice"); *Kirch v. Embarq Management Co.,* No. 10-2047-JAR, 2011 WL 3651359, at *7–9 (D. Kan. Aug. 19, 2011) (holding, in granting summary judgment for the defendant, that the plaintiffs consented to the use by third parties of their de-identified web-browsing behavior when they accessed the Internet under the terms of Embarq's Privacy Policy, which was incorporated by reference into its Activation Agreement, and which provided that de-identified information could be shared with third parties and that the Agreement could be modified; and because the Policy was amended in advance of the NebuAd test to expressly disclose the use and allow users to opt out by clicking on a hypertext link), *aff'd on other grounds*, 702 F.3d 1245 (10th Cir. 2012), *cert. denied*, 569 U.S. 1013 (2013); *Deering v. CenturyTel, Inc.*, No. CV-10-63-BLG-RFC, 2011 WL 1842859 (D. Mont. May 16, 2011) (dismissing plaintiff's ECPA claim based on the terms of defendant's privacy policy and an email sent to subscribers advising them that the Policy had been updated, in a putative class action suit over sharing of cookie and web beacon data); *Berry v. Webloyalty.com, Inc.*, No. 10-CV-1358-H CAB, 2011 WL 1375665, at *8 (S.D. Cal. Apr. 11, 2011) (in dismissing an ECPA claim over the "Shopper Discounts and Rewards" program, "[t]he Court conclude[d] that Plaintiff Berry's entry of his email address twice and clicking on 'YES' constitute[d] authorization given the several disclosures made on the enrollment page"), v*acated and remanded for lack of standing*, 517 F. App'x 581 (9th Cir. 2013); *Mortensen v. Bresnan Communication, LLC*, No. CV 10-13-BLG-RFC, 2010 WL 5140454 (D. Mont. Dec. 13, 2010) (dismissing plaintiff's ECPA claim where the defendant-ISP provided notice to consumers in its Privacy Notice and Subscriber Agreement that their electronic transmissions might be monitored and would in fact be transferred to third parties, and also provided specific notice via a link on its website of its use of the NebuAd Appliance to transfer data to NebuAd and of subscribers' right to opt out of the data transfer (via a link in that notice)), *vacated on other grounds*, 722 F.3d 1151 (9th Cir. 2013) (holding that the lower court erred in declin-

transit (or temporary, intermediate storage). In *In re iPhone Application Litigation*,[120] the court held that geolocation data stored for up to a one-year time period did not amount to "temporary, intermediate storage . . . incidental to the electronic transmission . . ." of an electronic communication.[121]

Title I claims also may fail where they are brought over information that is "readily accessible to the general public,"[122] such as material posted on a website[123] or on publicly accessible area of a social network profile page. In some cases, such as those involving social media, the information at issue was intended to be shared or was not otherwise actually private.

By contrast, the Ninth Circuit has held that payload data

---

ing to compel arbitration); *supra* § 26.14[2] (analyzing these cases). *But see In re Google Inc. Gmail Litig.,* Case No. 13–MD–02430–LHK, 2013 WL 5423918, at *12-15 (N.D. Cal. Sept. 26, 2013) (denying Google's motion to dismiss based on the court's finding that it did not have express or implied consent within the meaning of 18 U.S.C.A. § 2511(2)(d) to intercept incoming email to create profiles to send targeted advertising to recipients based on its Terms of Service and Privacy Policy); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1076–77 (N.D. Cal. 2012) (denying plaintiffs' motion to dismiss claims in a putative class action suit where the court found some ambiguity in the defendant's Terms and Conditions); *In re Vistaprint Corp. Marketing & Sales Practices Litig.*, MDL No. 4:08-md-1994, 2009 WL 2884727, at *9 (S.D. Tex. Aug. 31, 2009) (dismissing ECPA claim where plaintiffs, "by clicking Yes in the designated spaces on the webpages, authorized VistaPrint to transfer that information" to the "VistaPrint Rewards" program).

Consent also may be relevant to the issue of class certification. *See, e.g.*, *Sherman v. Yahoo! Inc.*, No. 13cv0041–GPC–WVG, 2015 WL 5604400 (S.D. Cal. Sept. 23, 2015) (denying class certification in a TCPA case based in part on individualized issues of consent); *In re Google Inc. Gmail Litigation*, Case No. 13–MD–02430–LHK, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014) (denying class certification because "consent must be litigated on an individual, rather than classwide basis.").

[120]*In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1059 (N.D. Cal. 2012).

[121]18 U.S.C.A. § 2510(17).

[122]*See* 18 U.S.C.A. § 2511(2)(g)(i) ("It shall not be unlawful under . . . chapter 121 of this title for any person—(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public . . . .").

[123]*See, e.g.*, *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1320–21 (11th Cir. 2006) (dismissing an SCA claim brought by an operator of an online bulletin board based on access to a website that was publicly accessible).

transmitted over unencrypted Wi-Fi networks that was inadvertently collected by Google on public roads, incident to capturing photographs for its free Street View service, was not "readily accessible to the public."[124]

Given the number of parties involved in online and mobile advertising, some suits have sought to hold defendants liable for third party practices. Where direct liability cannot be established under ECPA, however, civil claims may not be maintained based on aider and abettor, conspiracy or secondary liability.[125]

---

[124]*See Joffe v. Google, Inc.*, 746 F.3d 920, 926-35 (9th Cir. 2013) (affirming the district court's ruling that data transmitted over a Wi–Fi network is not a "radio communication" under the Wiretap Act, and thus could not qualify under the exemption for electronic communications that were "readily accessible to the general public"), *cert. denied*, 134 S. Ct. 2877 (2014); *see generally infra* § 44.06[1] (discussing the case and criticizing the Ninth Circuit's holding).

[125]*See, e.g.*, *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 168–69 (5th Cir. 2000), *cert. denied*, 532 U.S. 1051 (2001); *Doe v. GTE Corp.*, 347 F.3d 655, 658 (7th Cir. 2003) ("[N]othing in the statute condemns assistants, as opposed to those who directly perpetrate the act."); *Reynolds v. Spears*, 93 F.3d 428, 432–33 (8th Cir. 1996); *Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1005-06 (9th Cir. 2006) (affirming dismissal of plaintiff's Stored Communications Act claim and rejecting the argument that "a person or entity who aids and abets or who enters into a conspiracy is someone or something that is 'engaged' in a violation."); *Kirch v. Embarq Management Co.*, 702 F.3d 1245, 1246-47 (10th Cir. 2012) (holding that section 2520 "does not impose civil liability on aiders or abettors."), *cert. denied*, 569 U.S. 1013 (2013); *Satchell v. Sonic Notify, Inc.*, 234 F. Supp. 3d 996, 1007 (N.D. Cal. 2017) (holding that the plaintiff could not assert claims based on secondary liability; "Plaintiff has grouped the Defendants together and appears to argue she can establish liability by showing concerted action. However, in order to state a claim, Plaintiff must be able to allege that each Defendant engaged in conduct that directly violates the Wiretap Act."); *In re: Carrier IQ, Inc. Consumer Litig.*, 78 F. Supp. 3d 1051, 1089-90 (N.D. Cal. 2015) (dismissing plaintiffs' Wiretap Act claim where plaintiffs did not allege that the device manufacturers acquired the contents of any of plaintiffs' communications because "there is simply no secondary liability (such as aiding and abetting) under the ECPA"); *Byrd v. Aaron's, Inc.*, 14 F. Supp. 3d 667, 675 (W.D. Pa. 2014) (dismissing plaintiff's claim of conspiracy to commit ECPA violations because "secondary liability no longer exists under the current statutory structure of the ECPA."); *Shefts v. Petrakis*, 954 F. Supp. 2d 769, 774-76 (C.D. Ill. 2013) (granting summary judgment because "Defendant Morgan cannot be held liable under the ECPA under 'procurement,' 'agency,' 'conspiracy,' or any other 'secondary' theories of liability . . . ."); *Council on American-Islamic Relations Action Network, Inc. v. Gaubatz*, 891 F. Supp. 2d 13, 23–24 (D.D.C. 2012) (holding that there is no cause of action under ECPA for secondary li-

To state a civil claim for a violation of the Computer Fraud and Abuse Act (CFAA), a plaintiff must allege at least a $5000 loss,[126] which is a threshold that bars many consumer data privacy claims—especially those based on behavioral advertising where there is no economic loss or (injury) or merely *de minimis* damage. The $5,000 threshold requirement alone has proven to be an insurmountable bar in many data privacy cases.[127] Courts also have been reluctant to

---

ability, aiding and abetting liability or liability for procuring a primary violation (which existed prior to the 1986 amendments to the statute)); *Perkins-Carillo v. Systemax, Inc.*, No. 03-2836, 2006 WL 1553957 (N.D. Ga. May 26, 2006); *see generally infra* § 44.06[1].

[126]18 U.S.C.A. §§ 1030(c)(4)(A)(i), 1030(g). A civil CFAA claim where a $5,000 loss need not be shown may be made on limited grounds generally not applicable to data privacy cases. *See id.; infra* § 44.08[1] (analyzing the statutory provisions in greater detail).

[127]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 148-49 (3d Cir. 2015) (affirming dismissal of plaintiffs' CFAA claim for failure to allege the threshold loss of $5,000 required to state a civil claim under the CFAA, where they could not allege any viable lost marketing opportunity for their data), *cert. denied*, 137 S. Ct. 36 (2016); *Mount v. PulsePoint, Inc.*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *8-9 (S.D.N.Y. Aug. 17, 2016) (dismissing plaintiffs' CFAA claim in a suit based on alleged use of tracking cookies), *aff'd on other grounds*, 684 F. App'x 32 (2d Cir. 2017); *In re Google Android Consumer Privacy Litig.*, No. 11–MD–02264 JSW, 2014 WL 988889, at *4 (N.D. Cal. Mar. 10, 2014) (dismissing plaintiff's amended CFAA claim without leave to amend based on plaintiffs' inability to allege $5,000 in damages based on diminished battery life and data plan use); *In re Google Android Consumer Privacy Litig.,* No. 11-MD-02264, 2013 WL 1283236, at *7 (N.D. Cal. Mar. 26, 2013) (dismissing plaintiff's CFAA claim in a suit brought over the alleged sharing of information between the Android Market and advertisers, with leave to amend); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *10 (N.D. Cal. Mar. 26, 2013) (dismissing with leave to amend plaintiff's CFAA claim in a behavioral advertising putative class action suit where the plaintiff alleged diminished memory storage but did not allege $5,000 in damages); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1066–67 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' CFAA claim premised on the cost of memory space on class members' iPhones as a result of storing allegedly unauthorized geolocation data); *Del Vecchio v. Amazon.com, Inc.*, No. C11–366RSL, 2012 WL 1997697 (W.D. Wash. Jun. 1, 2012) (dismissing with prejudice plaintiff's CFAA claim for failure to allege $5,000 in damages); *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *4 (W.D. Wash. Dec. 1, 2011) (dismissing, with leave to amend, a CFAA claim based on the alleged use of browser and flash cookies for failure to allege $5,000 in damages or any injury, and questioning in *dicta* whether plaintiffs, in an amended complaint, could allege unauthorized access under the CFAA where the use of browser and flash cookies was disclosed to users in the

treat the disclosure of personal information as having economic value,[128] at least in the absence of any evidence to the

---

defendant's "Conditions of Use and Privacy Notice"); *Bose v. Interclick, Inc.,* No. 10 Civ. 9183, 2011 WL 4343517 (S.D.N.Y. Aug. 17, 2011) (dismissing with prejudice a CFAA claim alleging general impairment to the value of plaintiff's computer in a putative behavioral advertising class action suit); *LaCourt v. Specific Media, Inc.,* No. SACV 10-1256-GW (JCGx), 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011); *Czech v. Wall Street on Demand, Inc.*, 674 F. Supp. 2d 1102 (D. Minn. 2009) (dismissing a class action based on allegedly unauthorized text messages sent to plaintiffs' phones where plaintiffs merely alleged in conclusory fashion that the unwanted text messages depleted RAM and ROM, causing phone functions to slow down and lock up, caused phones to shut down, reboot or reformat their memory, interfered with bandwidth and hard drive capacity); *Fink v. Time Warner Cable,* No. 08 Civ. 9628 (LTS) (KNF), 2009 WL 2207920, at *4 (S.D.N.Y. July 23, 2009) (dismissing a CFAA claim because the plaintiff merely alleged damage by "impairing the integrity or availability of data and information," which was "insufficiently factual to frame plausibly the damage element of Plaintiff's CFAA claim"); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *see generally supra* § 5.06 (CFAA case law on database law and screen scraping); *infra* § 44.08 (analyzing the CFAA and case law construing it in greater detail).

In *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125 (3d Cir. 2015), *cert. denied*, 137 S. Ct. 36 (2016);, for example, plaintiffs alleged that their personally identifiable information was both 'currency' and a marketable 'commodity.' By capturing and making economic use of such information, the plaintiffs alleged, the defendants took the value of this information for themselves, depriving the plaintiffs of their own ability to sell information about their internet use, which caused them harm. *See id.* at 148-49. In rejecting these allegations as insufficient to state a claim under the CFAA, the Third Circuit explained:

> The complaint plausibly alleges a market for internet history information such as that compiled by the defendants. Further, the defendants' alleged practices make sense only if that information, tracked and associated, had value. However, when it comes to showing "loss," the plaintiffs' argument lacks traction. They allege no facts suggesting that they ever participated or intended to participate in the market they identify, or that the defendants prevented them from capturing the full value of their internet usage information for themselves. For example, they do not allege that they sought to monetize information about their internet usage, nor that they ever stored their information with a future sale in mind. Moreover, the plaintiffs do not allege that they incurred costs, lost opportunities to sell, or lost the value of their data as a result of their data having been collected by others. To connect their allegations to the statutory "loss" requirement, the plaintiffs' briefing emphasizes that lost revenue may constitute "loss" as that term is defined in the Act. This is inapposite, however, in that the plaintiffs had no revenue.

Id. at 149.

[128] *See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 148-49 (3d Cir. 2015) (affirming dismissal of plaintiffs' CFAA claim for failure to allege the threshold loss of $5,000 required to state a civil claim under the CFAA, where they could not allege any viable

contrary.

To state a CFAA claim, a plaintiff also must establish that a defendant accessed a protected computer "without authorization" or "exceeded authorized access."[129] At least in the Second, Fourth and Ninth Circuits, however, CFAA violations premised on use (rather than access) restrictions in a Privacy Policy, Terms of Use or company policy would not be viable.[130] As explained by the Second Circuit, a person exceeds authorized access "only when he obtains or alters information that he does not have authorization to access for any purpose which is located on a computer that he is otherwise authorized to access."[131] A person cannot exceed authorized access, within the meaning of the CFAA, by accessing a computer "with an improper purpose . . . . to obtain or alter information that he is otherwise authorized to access . . . . "[132]

Authorization similarly may be difficult to show in some data privacy cases where the plaintiff voluntarily downloaded the application that is challenged in the litigation.[133]

---

lost marketing opportunity for their data), *cert. denied*, 137 S. Ct. 36 (2016); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1068 (N.D. Cal. 2012); *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *3 (W.D. Wash. Dec. 1, 2011) (dismissing plaintiff's CFAA claim, with leave to amend, noting that "[w]hile it may be theoretically possible that Plaintiffs' information could lose value as a result of its collection and use by Defendant, Plaintiffs do not plead any facts from which the Court can reasonably infer that such devaluation occurred in this case."); *Bose v. Interclick, Inc.,* No. 10 Civ. 9183, 2011 WL 4343517, at *4 (S.D.N.Y. Aug. 17, 2011) (dismissing plaintiff's CFAA claim with prejudice; holding that "[t]he collection of demographic information does not constitute damage to consumers or unjust enrichment to collectors."); *In re Zynga Privacy Litig.,* No. C 10-04680 JWW, 2011 WL 7479170, at *3 (N.D. Cal. June 15, 2011) (dismissing plaintiffs' CFAA claim with prejudice where plaintiffs offered "no legal authority in support of the theory that personally identifiable information constitutes a form of money or property.").

[129]18 U.S.C.A. § 1030(a)(4); *see generally infra* § 44.08[1] (analyzing the CFAA in greater detail).

[130]*See U.S. v. Valle*, 807 F.3d 508, 524–28 (2d Cir. 2015); *WEC Carolina Energy Solutions, LLC v. Miller*, 687 F.3d 199, 203-06 (4th Cir. 2012), *cert. dismissed*, 568 U.S. 1079 (2013); *U.S. v. Nosal*, 676 F.3d 854, 856-63 (9th Cir. 2012) (*en banc*); *infra* § 44.08[1] (analyzing this issue in greater detail).

[131]*U.S. v. Valle*, 807 F.3d 508, 511 (2d Cir. 2015).

[132]*U.S. v. Valle*, 807 F.3d 508, 511 (2d Cir. 2015).

[133]*See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1066

In *In re iPhone Application Litigation*,[134] a CFAA claim was dismissed for the further reason that the allegation that Apple had failed to enforce its privacy policy against third party App providers, who made Apps available through Apple's iStore, was barred because a negligent software design cannot serve as the basis of a CFAA claim.[135]

Numerous putative class action suits have been filed under the Video Privacy Protection Act, which may be brought against a "video tape service provider who knowingly discloses, to any person, personally identifiable information" about the consumer.[136] However, an online video is not necessarily a *video tape.* The statutory definition of a *video tape service provider* appears to be limited to providers of audio visual and video works in tangible media, not works distributed electronically. The definition generally applies to any person engaged in the business of "rental, sales or delivery of prerecorded video cassette tapes or similar audio visual materials . . . ."[137] The Senate Report accompanying the bill clarifies that "similar audio visual materials" include such things as "laser discs, open -reel movies, or CDI technology . . . ,"[138] which was a technology for delivering movies on CD-like disks. All of these *materials* involve video stored

---

(N.D. Cal. 2012) (dismissing with prejudice plaintiffs' CFAA claim against the "iDevice class" premised on Apple's alleged practice of using iDevices to retain location history files because, among other things, plaintiffs voluntarily downloaded the software at issue and therefore Apple could not have accessed the devices without authorization); *see id.* at 1068 (dismissing with prejudice claims against the "geolocation class" where "the software or 'apps' that allegedly harmed the phone were voluntarily downloaded by the user . . . ."). In the *iPhone Application Litigation* case, the court noted in *dicta* that "Apple arguably exceeded its authority when it continued to collect geolocation data from Plaintiffs after Plaintiffs had switched the Location Services setting to 'off,' . . ." but dismissed plaintiffs' claim because they had sued for lack of authorization, not exceeding authorized access. *See id.* at 1066.

[134]*In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963 (N.D. Cal. Sept. 20, 2011).

[135]*In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963, at *11 (N.D. Cal. Sept. 20, 2011), *citing* 18 U.S.C. § 1030(g) ("No cause of action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.").

[136]*See* 18 U.S.C.A. § 2710(b)(1); *see generally supra* § 26.13[10].

[137]*See* 18 U.S.C.A. § 2710(a)(4).

[138]S. Rep. No. 100-599, 100th Cong. 2d Sess. 9, 12 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 3435-9 to 3435-10; *see generally supra*

on tangible media. Nevertheless, this argument about the inapplicability of the VPPA to online video players has not yet been addressed by any court.[139]

As analyzed more extensively in section 26.13[10], a VPPA suit will be unsuccessful where a plaintiff cannot establish a *knowing* disclosure,[140] if the information disclosed does not qualify as PII under the VPPA's statutory definition,[141] or because a cause of action under the VPPA may only be

---

§ 26.13[10] (expanding on this argument).

[139]*See generally supra* § 26.13[10] (analyzing case law in greater detail).

[140]*See, e.g.*, *Bernardino v. Barnes & Noble Booksellers, Inc.*, 17-CV-04570 (LAK) (KHP), 2017 WL 3727230, at *9 (S.D.N.Y. Aug. 11, 2017) (recommending that plaintiff's motion for a preliminary injunction be denied, in part, because the plaintiff had not demonstrated the likelihood of "proving that Barnes & Noble 'knowingly' made a disclosure of PII"); *In re: Hulu Privacy Litig.*, 86 F. Supp. 3d 1090 (N.D. Cal. 2015) (granting summary judgment for Hulu because there was no evidence of knowledge); *see generally supra* § 26.13[10] (analyzing the VPPA in greater detail).

[141]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262 (3d Cir. 2016) (holding that static digital identifiers (a user's IP address (which permits computer-specific tracking), "browser fingerprint" (a user's browser and operating system settings), and a computing device's unique device identifier), which allow for tracking a computer over time, did not constitute PII.), *cert. denied*, 137 S. Ct. 624 (2017); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 984-86 (9th Cir. 2017) (affirming dismissal of plaintiff's second amended complaint with prejudice because, while *personally identifiable information* under the VPPA covers "information that *can be used* to identify a person[,]" defendant's alleged disclosure of plaintiff's Roku device serial number and a record of videos he watched was not PII under the VPPA because it did not identify a specific person under the "ordinary person" test, focused on what was disclosed, not what a recipient might choose to do with the information); *Robinson v. Disney Online*, 152 F. Supp. 3d 176, 182 n.1 (S.D.N.Y. 2016) (dismissing plaintiff's VPPA claim because the encrypted serial number of the plaintiff's media-streaming device and plaintiff's video viewing history did not constitute *personally identifiable information*, which is information that "must itself do the identifying that is relevant for purposes of the VPPA . . . ;" it is "not information disclosed by a provider, plus other pieces of information collected elsewhere by non-defendant third parties."); *Locklear v. Dow Jones & Co.*, 101 F. Supp. 3d 1312, 1316-18 (N.D. Ga. 2015), *abrogated on other grounds by Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251 (11th Cir. 2015); *Ellis v. Cartoon Network, Inc.*, No. 1:14–cv–484–TWT, 2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014) (dismissing plaintiff's Video Privacy Protection Act claim because an Android ID is not "personally identifiable information"), *aff'd on other grounds*, 803 F.3d 1251 (11th Cir. 2015). *But see Yershov v. Gannett Satellite Information Network, Inc.*, 820 F.3d 482, 486 (1st Cir. 2016) (holding that a user's GPS coordinates and the Android

maintained for knowing disclosures, not the failure to delete information within the statutorily prescribed time limit[142] or for the receipt (rather than disclosure) of PII.[143] Several suits also have been dismissed because users of free mobile apps or website video players may not qualify as *consumers* eligible to sue under the statute (although there is a split of authority between the First and Eleventh Circuits on this point).[144]

Because alleged cloud-based, social media and mobile privacy claims often do not fit neatly within the confines of federal anti-hacking statutes or other federal criminal or narrow privacy laws, plaintiffs' lawyers may seek federal jurisdiction under the Class Action Fairness Act (CAFA).[145] Under CAFA, federal jurisdiction is permissible where more than two-thirds of the members of the putative class are alleged to be citizens of states other than that of the named plaintiff and the amount of damages alleged exceeds $5 mil-

---

ID of a user's smart phone plausibly constituted PII under the VPPA); *see generally supra* § 26.13[10] (analyzing these cases).

[142]*See, e.g.*, *Daniel v. Cantrell*, 375 F.3d 377, 384-85 (6th Cir. 2004) (holding that "only § 2710(b) can form the basis of liability."); *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535, 538-39 (7th Cir. 2012); *Rodriguez v. Sony Computer Entertainment America*, LLC, 801 F.3d 1045, 1050-53 (9th Cir. 2015); *see generally supra* § 26.13[10] (analyzing these cases).

[143]*See In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 279-81 (3d Cir. 2016) (holding that Google could not be held liable under the VPPA for allegedly receiving certain information from cookies placed by Viacom on plaintiff's computers because "only video tape service providers that disclose personally identifiable information can be liable under subsection (c) of the Act . . . ."), *cert. denied*, 137 S. Ct. 624 (2017).

[144]A *consumer* is "any renter, purchaser, or subscriber of goods or services from a video tape service provider . . . ." 18 U.S.C.A. § 2710(a)(1). Users of free services are not renters or purchasers and frequently may not qualify as *subscribers* if they merely downloaded a free app or visited a website. *See, e.g.*, *Perry v. CNN*, 854 F.3d 1336, 1341-44 (11th Cir. 2017); *Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251, 1255-58 (11th Cir. 2015); *Austin-Spearman v. AMC Network Entertainment LLC*, 98 F. Supp. 3d 662, 669 (S.D.N.Y. 2015). *But see Yershov v. Gannett Satellite Information Network, Inc.*, 820 F.3d 482, 489 (1st Cir. 2016) (holding that a plaintiff who downloaded *USA Today*'s mobile app to his Android device to watch news and sports video clips, plausibly stated a claim that he was a *subscriber* because in downloading the app he gave Gannett the GPS location of his mobile device, his device identifier and the titles of the videos he viewed in return for access to Gannett's video content); *see generally supra* § 26.13[10] (analyzing the VPPA in greater detail).

[145]28 U.S.C.A. § 1332(d).

lion dollars. Even where plaintiff's counsel alleges the existence of a class of millions of people, the $5 million bar may be difficult to meet in a case where there has been no economic injury. If the named plaintiffs cannot meet the $5,000 threshold to state a CFAA claim, for example, a potential class of similarly situated parties who also have not been injured may not meet CAFA's $5 million threshold.[146]

State law claims may suffer from some of the same defects as federal claims in cases where there is no injury or actual damage or where consent has been obtained or notice provided in Terms of Use or a Privacy Policy. For example, to maintain a state law breach of contract claim, plaintiffs generally must be able to plead and prove actual injury and damage[147] (although in the Ninth Circuit plaintiffs theoretically may be able to plead diminishment of the market value

---

[146]*See* Ian C. Ballon & Wendy Mantell, *Suing Over Data Privacy and Behavioral Advertising*, ABA Class Actions, Vol. 21, No. 4 (Summer 2011).

[147]*See, e.g.*, *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301, at *16 (N.D. Cal Dec. 21, 2016) (granting summary judgment in favor of Google on plaintiff's individual claims for breach of contract and breach of the duty of good faith and fair dealing because the plaintiff could present no evidence of damages from Google's alleged (but disputed) breach of its privacy policy); *Svenson v. Google Inc.*, 65 F. Supp. 2d 717, 724–25 (N.D. Cal. 2014) (dismissing plaintiff's breach of contract claim with leave to amend for failing to sufficiently allege damage where "Plaintiff has not alleged any facts showing that Defendants' business practice—disclosing users' Contact Information to third-party App vendors—changed her economic position at all."); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *13 (N.D. Cal. Mar. 26, 2013) (dismissing plaintiff's breach of privacy policy claim with leave to amend where the plaintiff failed to allege "actual and appreciable damage based on the collection and dissemination of his PII."); *Rudgayzer v. Yahoo! Inc.,* No. 5:12-CV-01399 EJD, 2012 WL 5471149, at *7 (N.D. Cal. Nov. 9, 2012) (dismissing plaintiff's suit alleging breach of contract because his first and last name was disclosed in the "from" line of his Yahoo! email account where "an allegation of the disclosure of personal or private information does not constitute actionable damage for a breach of contract claim."); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1028-29 (N.D. Cal. 2012) (dismissing plaintiffs' contract claim with prejudice because emotional and physical distress damages are not recoverable for breach of contract under California law and because the unauthorized collection of personal information does not create economic loss and plaintiffs did not allege that the collection foreclosed their opportunities to capitalize on the value of their personal information or diminished its value); *In re Zynga Privacy Litig.,* No. C 10-04680 JWW, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011) (dismissing plaintiffs' breach of contract claim because California law requires a showing of "appreciable harm and actual damage" to assert such a claim).

of personal information[148]). A claim likewise may fail based on the language of the Privacy Policy.[149]

Although numerous putative class action suits were brought against subscription music services and magazine vendors under Michigan's Preservation of Personal Privacy Act (a part of which is also known as Michigan Video Rental Privacy Act), which previously afforded a successful plaintiff up to $5,000 in statutory damages, that statute was amended effective July 31, 2016, to no longer provide a statutory damages remedy.[150] As a consequence, for claims brought on or

---

[148]*See In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014) (reversing dismissal of plaintiffs' breach of contract claim because alleging that plaintiffs "were harmed both by the dissemination of their personal information and by losing the sales value of that information" was sufficient to state a claim under California law), *rev'g*, 791 F. Supp. 2d 705, 717 (N.D. Cal. 2011) (dismissing plaintiffs' contract claim because the unauthorized collection of information by a third party does not amount to an economic loss); *Svenson v. Google Inc.*, Case No. 13–cv–04080–BLF, 2015 WL 1503429, at *4-5 (N.D. Cal. Apr. 1, 2015) (denying defendant's motion to dismiss breach of contract claim under the benefit of the bargain and diminution of value of personal information theories, where the plaintiff alleged (1) a contract for each Google Wallet transaction whereby she would receive payment processing service that would facilitate her Play Store purchase while keeping her private information confidential in all but specific circumstances under which disclosure was authorized, and (2) the existence of a market for personal information where the value of her information was diminished by Google's alleged use).

Some of the theories alleged by plaintiffs' counsel to survive motions to dismiss would likely be difficult if not impossible to prove at trial or on summary judgment. *See, e.g.*, *Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301, at *16 (N.D. Cal Dec. 21, 2016) (granting summary judgment in favor of Google on plaintiff's individual claims for breach of contract and breach of the duty of good faith and fair dealing, after earlier denying defendant's motion to dismiss, as noted earlier in this footnote, because "even if Google did breach its Privacy Policies, Svenson has presented no evidence of resulting damages."); *see also Yunker v. Pandora Media, Inc.*, No. 11–CV–03113 JSW, 2014 WL 988833, at *5 (N.D. Cal. Mar. 10, 2014) (denying defendant's motion to dismiss plaintiff's amended breach of contract claim, but noting that "Plaintiffs may face an uphill battle proving this claim").

[149]*See, e.g., Carlsen v. GameStop, Inc.*, 833 F.3d 903, 910-12 (8th Cir. 2016) (affirming dismissal of plaintiff's claims for breach of contract and alleged violations of Minnesota's Consumer Fraud Act, where GameStop's Privacy Policy, which was incorporated in its Terms of Service, did not define PII to include plaintiff's Facebook ID and browser history, which were the data elements that plaintiff alleged had been improperly shared).

[150]*See* Mich. Comp. Laws § 445.1715(2) (limiting claims to "customers . . . . who [have] suffer[ed] actual damages . . . . "); *see generally supra*

after July 31, 2016, a plaintiff cannot state a claim if he she

---

§ 26.13[10] (analyzing the statute and discussing cases construing it). Mich. Comp. Laws Ann. § 445.1712(1) generally provides that, "except otherwise as provided by law, a person, or an employee or agent of the person, engaged in the business of selling at retail, renting, or lending books or other written materials, sound recordings, or video recordings shall not knowingly disclose to any person, other than the customer, a record or information that personally identifies the customer as having purchased, leased, rented, or borrowed those materials from the person engaged in the business." The statute creates an exception for "the disclosure of a record or information that has been aggregated or has been processed in a manner designed to prevent its association with an identifiable customer." *Id.* §§ 445.1712(1), 445.1712(2).

The statute also permits disclosure (a) with the written permission of the customer, (b) pursuant to a warrant or court order, (c) "to the extent reasonably necessary to collect payment for the materials or the rental of the materials, if the customer has received written notice that the payment is due and has failed to pay or arrange for payment within a reasonable time after notice," (d) to any person, for a record or information "created or obtained" after July 31, 2016, if the disclosure is "incident to the ordinary course of business of the person that is disclosing the record or information," (e) for the purpose of marketing goods and services to customers, but only if a series of specific notice requirements set forth in section 445.1713(e) have been met, or (f) pursuant to a search warrant issued by a state or federal court or a grand jury subpoena. *Id.* § 445.1713.

For marketing goods or services to consumers, disclosure is only permitted if the person disclosing the information informs the customer by written notice that the customer may remove his or her name at any time and specifies the manner(s) by which the customer may do so. "Unless the person's method of communication with customers is by electronic means, the written notice shall include a nonelectronic method that the customer may use to opt out of disclosure." *Id.* § 445.1713(e)(i). Otherwise, the notice requirement may be met by:

> (A) Written notice included in or with any materials sold, rented, or lent to the customer under section 2.
>
> (B) Written notice provided to the customer at the time he or she orders any of the materials described in section 2 or otherwise provided to the customer in connection with the transaction between the person and customer for the sale, rental, or loan of the materials to the customer.
>
> (C) Notice that is included and clearly and conspicuously disclosed in an online privacy policy or similar communication that is posted on the Internet, is maintained by the person that is disclosing the information, and is available to customers or the general public.

Id. Customers have the right to provide notice that they do not wish to have their names disclosed. *Id.* § 445.1713(e)(ii). When such a notice is provided, a person may not "knowingly disclose the customer's name to any other person for marketing goods and services" beginning 30 days after receipt of the notice. *Id.* § 445.1713(e)(iii).

A customer who "suffers actual damages as a result of a violation" of this PPPA may bring a civil action against the person that violated this

did not suffer actual damages.[151]

A claim under the Illinois Biometric Information Privacy Act (BIPA)[152] likewise may fail where the plaintiff cannot establish that he or she is *aggrieved by* the alleged violation.[153]

---

act and recover (a) "actual damages, including damages for emotional distress" and (b) reasonable costs and attorneys' fees. *Id.* § 445.1715(2).

[151]*See Raden v. Martha Stewart Living Omnimedia, Inc.,* Case No. 16-12808, 2017 WL 3085371, at *3-4 (E.D. Mich. July 20, 2017) (dismissing plaintiff's claim, filed on July 31, 2016, because plaintiff had not alleged actual damages).

[152]740 Ill. Comp. Stat. Ann. 14/1 to 14/25; *see generally supra* § 26.13[12] (analyzing the statute).

[153]*See* 740 Ill. Comp. Stat. Ann. 14/20 (authorizing a private right of action for "any person aggrieved by a violation" of BIPA); *Rosenbach v. Six Flags Entertainment Corp.*, 2017 Il. App. (2d) 170317, __ N.E.3d __ (2d Dist. 2017) (holding that a child who had been fingerprinted in connection with his mother's purchase of a season pass for a theme park had suffered only a "technical violation" of the Act and was not "aggrieved"); *Vigil v. Take-Two Interactive Software, Inc.*, 235 F. Supp. 3d 499, 510-21 (S.D.N.Y. 2017) (dismissing plaintiff's amended complaint with prejudice, holding that players of Take-Two's NBA 2K15 video game, which scanned players' faces, did not have either Article III or statutory standing to sue for alleged violations of BIPA because plaintiffs' alleged failure to comply with provisions regulating the storage and dissemination of biometric information and requiring notice and consent to the collection of biometric information amounted to merely "procedural violations" under *Spokeo*, where plaintiffs conceded that they "received advance notice that their faces would be scanned . . . . [and] consented to have their faces scanned," and a "more extensive notice and consent could not have altered the standing equation because there has been no material risk of harm to a concrete BIPA interest that more extensive notice and consent would have avoided" where the defendant used the biometic data as intended by the parties), *aff'd on other grounds sub. nom Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12 (2d Cir. 2017) (affirming dismissal based on lack of Article III standing without reaching the statutory standing issue); *McCollough v. Smarte Carte, Inc.*, Case No. 16 C 03777, 2016 WL 4077108, at *4 (N.D. Ill. Aug. 1, 2016) (dismissing plaintiff's putative Illinois Biometric Information Privacy Act class action suit for lack of Article III and statutory standing where the plaintiff alleged that Smarte Carte retained her fingerprint biometric information without written consent, where Smarte Carte used a person's fingerprints to allow them to access a rented locker, because, with respect to statutory standing, she could not establish that she was "aggrieved by" the alleged violation, to establish statutory standing). *But see Dixon v. Washington and Jane Smith Community—Beverly*, Case No. 17 C 8033, 2018 WL 2445292, at *11-12 (N.D. Ill. May 31, 2018) (denying defendant's motion to dismiss for lack of statutory standing as a "person aggrieved" because "Dixon did allege an injury to a privacy right in her complaint—and . . . obtaining or disclosing a person's biometric data without her consent or knowledge constitutes an

actual and concrete injury because it infringes on the right to privacy in that data . . . ."); *In re Facebook Biometric Information Privacy Litig.*, __ F.R.D. __, 2018 WL 1794295, at *7-8 (N.D. Cal. 2018) (disagreeing with *Rosenbach* and holding that plaintiffs established that they were "aggrieved" merely by establishing an alleged statutory violation); *Munroy v. Shutterfly, Inc.*, Case No. 16 C 10984, 2017 WL 4099846, at *8 & n.5 (N.D. Ill. Sept. 15, 2017) (distinguishing *Vigil* and *McCollough* as cases where plaintiffs voluntarily provided their biometric data to defendants; "Munroy, by contrast, alleges the he had no idea that Shutterfly had obtained his biometric data in the first place. Thus, in addition to any violation of BIPA's disclosure and informed consent requirements, Munroy also credibly alleges an invasion of privacy."); *Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 Il. App (1st) 180175, __ N.E.3d __ (2018) (reversing the lower court's holding that the plaintiff had not been aggrieved, in a case where the plaintiff alleged that defendant violated BIPA by collecting her fingerprints without providing the statutorily required disclosures and by disclosing her fingerprints to an out-of-state vendor).

Some courts, however, have broadly construed the statute in denying motions to dismiss, without addressing statutory or Article III standing. *See e.g., Munroy v. Shutterfly, Inc.,* Case No. 16 C 10984, 2017 WL 4099846, at *2-5 (N.D. Ill. Sept. 15, 2017) (denying Shutterfly's motion to dismiss because even though data extracted from plaintiff's photograph could not constitute "biometric information" within the meaning of the statute because photographs are expressly excluded from the definition of *biometric identifier* and the definition of *biometric information* expressly excludes "information derived from items or procedures excluded under the definition of biometric identifiers," the inclusion of "face geometry" in the definition of "biometric identifier" means that this data, derived from a photograph, is covered by the statute); *Rivera v. Google Inc.,* 238 F. Supp. 3d 1088, 1092-1100 (N.D. Ill. 2017) (holding that plaintiff sufficiently alleged that face templates created from uploaded photographs depicting plaintiffs were biometric indicators under BIPA and that the face templates were created in Illinois, justifying application of BIPA); *In re Facebook Biometric Information Privacy Litig*., 185 F. Supp. 3d 1155, 1170-72 (N.D. Cal. 2016) (denying defendant's motion to dismiss plaintiffs' claims brought over Facebook's "Tag suggestions program" which, using facial recognition technology, allegedly extracted biometric identifiers from user uploaded photographs, even though the statute, on its face, excludes from the definitions of *biometric identifier* and *biometric information* photographs and any information derived from those photographs, based on a broad reading of the statute which narrowly limited the exclusion for photographs to paper prints, not digital images); *Norberg v. Shutterfly, Inc.*, 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015) (denying defendants' motion to dismiss the claim of a plaintiff, who was not a user of either Shutterfly.com or ThisLife.com and was never presented with a written biometrics policy and did not consent to have his biometric identifiers used by defendants, under the Illinois Biometric Information Privacy Act, where defendants allegedly used facial recognition technology to identify and categorize photos based on the people pictured in the photos, including the plaintiff); *see generally supra* § 26.13[12] (analyzing privacy in biometric and genetic data).

Plaintiffs also have sought to sue online genetic testing companies under state genetic privacy statutes.[154] While a number of states have enacted laws protecting privacy in genetic data, only a limited number provide for a private cause of action.[155]

A claim for breach of the implied duty of good faith and fair dealing based on privacy violations may similarly be defective if the claim is merely duplicative of a plaintiff's breach of contract claim or contradicted by the plain terms of the contract.[156]

State computer crime statutes may not provide grounds for relief in a case where there has been no economic harm.[157]

---

[154]*See, e.g., Cole v. Gene By Gene, Ltd.,* Case No. 1:14-cv-00004-SLG, 2017 WL 2838256 (D. Alaska June 30, 2017) (denying defendant's motion to dismiss, holding that the plaintiff had Article III standing to sue over the alleged release of his DNA test kit results by the owner of familytreedna.com in a putative class action suit alleging violations of the Alaska Genetic Privacy Act).

[155]*See, e.g.,* Alaska Stat. § 18.13.020 (providing for actual damages plus $5,000 or, if the violation resulted in profit or monetary gain to the violator, $100,000); N.J. Stat. Ann. § 10:5-49(c) (providing for the recovery of actual damages, including damages for economic, bodily, or emotional harm, proximately caused by the disclosure of an individual's genetic information in violation of New Jersey's Genetic Privacy Act); N.M. Stat. Ann. § 24-21-6 (allowing for recovery of actual damages, damages of up to $5,000 in addition to any economic loss if the violation results from willful or grossly negligent conduct, and reasonable attorneys' fees, among other things); Or. Rev. Stat. Ann. § 192.541 (providing for a range of statutory damages); Utah Code Ann. § 26-45-105 (allowing for injunctive relief and damages, plus statutory and punitive damages against an insurance company or employer who violates the Genetic Testing Privacy Act); *see generally supra* § 26.13[12] (analyzing privacy in biometric and genetic data).

[156]*See, e.g., Svenson v. Google Inc.*, 65 F. Supp. 2d 717, 725-26 (N.D. Cal. 2014) (dismissing plaintiff's breach of the implied duty of good faith and fair dealing claim as duplicative of her breach of contract claim); *see also Song Fi Inc. v. Google, Inc.*, 108 F. Supp. 3d 876, 885 (N.D. Cal. 2015) (granting Google's motion to dismiss claims for breach of YouTube's Terms of Service and breach of the duty of good faith and fair dealing arising out of plaintiffs' removal of a video where the Terms of Service permitted YouTube to remove the video "and eliminate its view count, likes, and comments"; "if defendants were given the right to do what they did by the express provisions of the contract there can be no breach [of the duty of good faith and fair dealing].").

[157]*See, e.g., In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 277-78 (3d Cir. 2016) (affirming the district court's dismissal with prejudice of plaintiffs' claims under the New Jersey Computer Related Offenses

Even specialized statutes intended to make it easy for plaintiff's counsel to bring consumer class action cases may not be well suited to data privacy suits based on behavioral advertising or other perceived privacy violations where there is no quantifiable harm or only *de minimis* damage. For example, California's Consumer Legal Remedies Act (CLRA),[158] which provides a potential remedy to consumers for damages suffered in connection with a consumer transaction, defines a *consumer* as an individual who purchases or leases any goods or services for personal, family or household purposes.[159] A CLRA claim therefore may not be maintained where a plaintiff seeks a remedy from a free Internet site or free app where no purchase has been made,[160] although a

---

Act (CROA), N.J. Stat. Ann. § 2A:38A–3, an anti-hacking statute, because plaintiffs could not "allege that they had been 'damaged in business or property,' as the plain text of the New Jersey Act requires" and because the appellate panel was not willing to "credit their theory of damage—namely, that the defendants' appropriation of their personal information, without compensation, constituted unjust enrichment . . . [even though] plaintiffs concede that 'unjust enrichment has never been used as a measure of damages' under the New Jersey Act . . . ."), *cert. denied*, 137 S. Ct. 624 (2017). The Third Circuit reiterated that merely alleging, as plaintiffs did in this case, that the defendant gained access to information is not sufficient; a plaintiff must present "proof of some activity vis-à -vis the information other than simply gaining access to it." *Id.* at 277, *quoting P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 509 (3d Cir. 2005). In addition, New Jersey courts, the panel noted, construe the statute as requiring the same type of evidence of damage as that required by the federal Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030. *See In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 278 (3d Cir. 2016), *cert. denied*, 137 S. Ct. 624 (2017).

[158]Cal. Civil Code §§ 1750 *et seq.*; *see generally supra* § 25.04[3] (analyzing the statute).

[159]*Schauer v. Mandarin Gems of California, Inc.*, 125 Cal. App. 4th 949, 960, 23 Cal. Rptr. 3d 233 (4th Dist. 2005).

[160]*See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 152-53 (3d Cir. 2015) (affirming dismissal of plaintiffs' CLRA claim and rejecting the argument that Google's alleged access to personal information stored in cookies constituted a forced "sale" of trackable internet history information as a form of payment to Google), *cert. denied,* 137 S. Ct. 36 (2016); *In re Yahoo! Inc. Customer Data Security Breach Litig.*, No. 16-MD-02752-LHK, 2017 WL 3727318, at *32-33 (N.D. Cal. Aug. 30, 2017) (dismissing plaintiffs'CLRA claim because "[t]he mere fact that Yahoo gained some profit from Plaintiffs' use of Yahoo's free email services does not by itself show that Plaintiffs 'purchased' those services from Defendants. . . . Plaintiffs cite no legal authority—and the Court is not aware of any legal authority—to support Plaintiffs' theory that the mere transfer of PII renders Plaintiffs' use of a free service a 'purchase' or

Ninth Circuit panel, in an unreported decision, allowed a CLRA claim to proceed premised on the lost sales value of personal information.[161] Some courts have also suggested that a CLRA claim may not be made when based on the collection of information by software, as opposed to the sale of goods or services.[162] A CLRA claim also may fail where the plaintiffs cannot allege reliance (for example, when a CLRA claim is premised on the breach of a privacy policy).[163]

'lease' of that service. . . . The Court cannot ignore the CLRA's 'strict requirement' of a 'purchase or lease' simply because Plaintiffs believe that the result is unfair in this case."); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *12 (N.D. Cal. Mar. 26, 2013) (rejecting the argument that the plaintiff "purchased" Pandora's services by providing his PII and holding that plaintiff failed to allege he was a "consumer" within the meaning of the CLRA; granting Pandora's motion to dismiss with leave to amend); *In re Zynga Privacy Litig.,* No. C 10-04680 JWW, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011) (dismissing plaintiffs' CLRA claim, with leave to amend, because a CLRA claim may only be brought by someone who purchases or leases goods or services but the plaintiff alleged that the defendant's services were offered for free). *But see In re Sony Gaming Networks and Customer Data Security Breach Litig.*, 996 F. Supp. 2d 942, 992 (S.D. Cal. 2014) (holding that a CLRA claim arising out of a security breach of the PlayStation Network could not be premised on plaintiffs' registration for this free service, but could proceed based on omissions about the security of the service at the time they purchased their PlayStation consoles (a good)); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1070 (N.D. Cal. 2012) (denying defendants' motion to dismiss where plaintiffs in a data privacy putative class action suit, in their amended complaint, did not merely allege that free apps failed to perform as represented but that the value of their iPhones (a good) would have been materially lower if defendants had disclosed how the free apps in fact allegedly operated).

[161] *See In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014) (reversing dismissal with prejudice of plaintiffs' CLRA claim where plaintiffs alleged injuries from the lost sales value of personal information allegedly disseminated to advertisers).

[162] *See, e.g.*, *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *13 (N.D. Cal. Mar. 26, 2013) (holding that the Pandora app was not a "good" for purposes of the CLRA); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1070 (N.D. Cal. 2012) (citing an earlier case for the proposition that software is neither a good nor a service under the CLRA); *In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963, at *10 (N.D. Cal. Sept. 20, 2011) (same).

[163] *See In re Google, Inc. Privacy Policy Litigation*, 58 F. Supp. 3d 968, 982-83 (N.D. Cal. 2014) (dismissing with prejudice plaintiffs' CLRA claim, explaining that "[i]f Nisenbaum and the other members of his subclass did not see, read, hear or consider the terms of Google's then-active privacy policy before creating their account, they could not have relied on any representation it contained in making their decisions to purchase Android

Claims under California's Invasion of Privacy Act (CIPA)[164] or the California Constitution[165] likewise will not be actionable, as under ECPA, if premised on non-content data, as opposed to the contents of communications.[166] A CIPA claim likewise may not be maintained where the defendant itself was a party to the alleged communication.[167] California

---

phones, and without affirmatively alleging reliance on Google's misrepresentations, the CLRA claim cannot survive.").

[164]California's Invasion of Privacy Act (CIPA), Penal Code § 630, affords a cause of action where a defendant "willfully and without the consent of all parties to the communication, or in any unauthorized manner," intercepted, used, or disclosed the "contents or meaning" of a "communication" that is "in transit." Cal. Penal Code § 631(a); *In re Facebook Internet Tracking Litig.*, 263 F. Supp. 3d 836, 845 (N.D. Cal. 2017) (dismissing plaintiff's CIPA claims under sections 631 and 632 because Facebook did not intercept data or eavesdrop); *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 937 (N.D. Cal. 2015) (dismissing plaintiff's CIPA claim where he did not plead facts to show how Facebook used a "machine, instrument or contrivance" to obtain the contents of communications and did not adequately allege that Facebook acquired the contents of a communication); *NovelPoster v. Javitch Canfield Group*, 140 F. Supp. 3d 938, 953–54 (N.D. Cal. 2014) (dismissing plaintiff's CIPA claim based on allegations that defendants "wrongfully accessed the accounts at issue," because "any subsequent reading or forwarding of those emails by defendants does not constitute an illegal 'interception' ").

Section 632 provides an additional potential claim against any "person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication." Courts have rejected claims brought under section 632 for the disclosure of information, however, where a party to the communication does not have an objectively reasonable expectation of privacy, including Internet communications. *See, e.g.*, *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 848-49 (N.D. Cal. 2014) (dismissing plaintiff's claim based on allegedly scanned Facebook messages); *In re Google Inc. Gmail Litig.*, Case No. 13–MD–02430–LHK, 2013 WL 5423918, at *23 (N.D. Cal. Sept. 26, 2013) (scanned email); *see also People v. Nakai*, 183 Cal. App. 4th 499, 518, 107 Cal. Rptr. 3d 402 (2010) (holding internet chat to not be confidential).

[165]*See supra* § 26.07[2] (analyzing the contours of California's Constitutional right to privacy, as set forth in Article I, Section 1 of the California Constitution).

[166]*See In re Yahoo Mail Litigation*, 7 F. Supp. 3d 1016, 1037-42 (N.D. Cal. 2014) (dismissing with leave to amend plaintiff's claim for a violation of California's constitutional right to privacy where plaintiffs alleged that Yahoo's alleged scanning, storage and disclosure of email content violated their right to privacy).

[167]*See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 152 (3d Cir. 2015) (affirming dismissal of plaintiffs' CIPA

privacy claims also may not be viable where consent has been obtained[168] or where a privacy violation is not substantial.[169]

Similarly, California's notoriously-broad unfair competition statute requires a showing of actual injury. That statute—California Business and Professions Code section 17200[170]—allows claims to be based on violations of statutes that do not expressly create independent causes of action.[171] Indeed, under section 17200, "[u]nlawful acts are 'anything that can properly be called a business practice and that at the same time is forbidden by law . . . be it civil, criminal, federal, state, or municipal, statutory, regulatory, or court-made,' where court-made law is, 'for example a violation of a prior court order.' "[172] A claim under section 17200, however, may not be made absent a showing that a plaintiff "suffered injury in fact and has lost money or property as a result of

---

claim because Cal. Penal Code § 631(a), like the Wiretap Act, broadly prohibits the interception of wire communications and disclosure of those intercepted communications—*i.e.*, eavesdropping or the secret monitoring by third parties—and could not be applied to Google's alleged use and disclosure of information stored in cookies because Google was itself a party to those electronic communications), *cert. denied*, 137 S. Ct. 36 (2016).

[168]*See Garcia v. Enterprise Holdings, Inc.*, 78 F. Supp. 3d 1125, 1135-37 (N.D. Cal. 2015) (dismissing plaintiff's California Invasion of Privacy Act claim with leave to amend where the defendant—app provider's Terms of Use and Privacy Policy provided consent for the alleged disclosures).

[169]*See, e.g., Yunker v. Pandora Media, Inc.*, No. 11–CV–03113 JSW, 2014 WL 988833, at *5-6 (N.D. Cal. Mar. 10, 2014) (dismissing with prejudice plaintiff's claim under the California Constitution based on their inability to allege conduct that was "sufficiently serious in [its] nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right."; citation omitted); *see generally supra* § 26.07[2] (analyzing the California Constitutional right to privacy).

[170]Cal. Bus. & Prof. §§ 17200 *et seq.*

[171]*See, e.g.*, *Kasky v. Nike, Inc.*, 27 Cal. 4th 939, 950, 119 Cal. Rptr. 2d 296, 304 (2002); *Stop Youth Addiction, Inc. v. Lucky Stores, Inc.*, 17 Cal. 4th 553, 561–67, 71 Cal. Rptr. 2d 731, 736–40 (1998); *see generally supra* § 25.04[3].

[172]*Sybersound Records, Inc. v. UAV Corp.*, 517 F.3d 1137, 1151–52 (9th Cir. 2008), *citing National Rural Telecommunications Co-op. v. DIRECTV, Inc.*, 319 F. Supp. 2d 1059, 1074 n.22 (C.D. Cal. 2003) (quoting *Smith v. State Farm Mutual Automobile Ins. Co.*, 93 Cal. App. 4th 700, 113 Cal. Rptr. 2d 399, 414 (2d Dist. 2001); *Saunders v. Superior Court*, 27 Cal. App. 4th 832, 33 Cal. Rptr. 2d 438, 441 (2d Dist. 1994) (internal quotations omitted)).

such unfair competition."[173] Hence, a plaintiff generally may not maintain suit for privacy violations where the plaintiff obtained access to the defendant's service free of charge[174] unless the claim may be premised on the value of a product purchased in conjunction with obtaining free services[175] or potentially for breach of a statutory duty to adhere to the

---

[173]Cal. Bus. & Prof. Code § 17200. "An injury in fact is '[a]n actual or imminent invasion of a legally protected interest, in contrast to an invasion that is conjectural or hypothetical." *Hall v. Time Inc.*, 158 Cal. App. 4th 847, 853, 70 Cal. Rptr. 3d 466, 470 (4th Dist. 2008). A plaintiff must show loss of money or property to have standing to seek injunctive relief or restitution. *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 323-34, 336, 120 Cal. Rptr. 3d 741 (2011); *see generally supra* § 6.12[6] (analyzing section 17200).

[174]*See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 152 (3d Cir. 2015) (affirming dismissal of plaintiffs' 17200 claim based on Google's alleged collection of data stored in Internet cookies), *cert. denied*, 137 S. Ct. 36 (2016); *In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal with prejudice of plaintiffs' UCL claim where plaintiffs could not allege that they "lost money or property as a result of the unfair competition."), *aff'g*, 791 F. Supp. 2d 705, 714-15 (N.D. Cal. 2011) (dismissing with prejudice plaintiffs' UCL claim where plaintiffs alleged that the defendant unlawfully shared their "personally identifiable information" with third-party advertisers because personal information does not constitute property for purposes of a UCL claim; "Because Plaintiffs allege that they received Defendant's services for free, as a matter of law, Plaintiffs cannot state a UCL claim."); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *11 (N.D. Cal. Mar. 26, 2013) (dismissing plaintiff's claim with leave to amend where the plaintiff alleged that his PII was diminished in value based on Pandora's alleged use); *In re Zynga Privacy Litig.,* No. C 10-04680 JWW, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011) (dismissing plaintiffs' UCL claim, with leave to amend, where plaintiffs did not allege that they lost money as a result of defendants' conduct, but instead merely alleged that defendants shared their personally identifiable information with third party advertisers).

[175]*See Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301, at *16-17 (N.D. Cal Dec. 21, 2016) (granting summary judgment in favor of Google on plaintiff's 17200 claim for lack of statutory standing as well as lack of Article III standing, where "the Google services used by Svenson were free, and she has failed to show that she paid Google any money. To the extent that Svenson entered into a bargain with Google to buy an App on Google's platform in exchange for privacy protections, the asserted loss of those privacy protections does not constitute a loss of *money* or *property*."); *Svenson v. Google Inc.*, 65 F. Supp. 2d 717, 730 (N.D. Cal. 2014) (dismissing plaintiff's UCL claim with leave to amend for failure to allege economic injury); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1071–74 (N.D. Cal. 2012) (denying defendants' motion to dismiss in a data privacy putative class action suit where plaintiffs, in their amended complaint, did not merely allege a UCL violation based on alleged information

terms of a company's privacy policy.[176] Courts have also rejected the argument that plaintiffs have a property interest in their personal information or electronic communications that amounts to lost property under section 17200.[177] Since many Internet sites and services provide free access, this restriction limits potential unfair competition claims against many of the more popular Internet and social media sites.

Absent injury, statutory unfair competition claims under the laws of other states similarly may not be viable.[178]

---

gathering in connection with free apps, but asserted that they purchased their mobile devices based on the availability of thousands of free apps, but would not have done so if the true value of the devices had been disclosed by revealing that the apps allegedly allowed third parties to collect consumers' information).

[176]*See Svenson v. Google Inc.*, Case No. 13–cv–04080–BLF, 2015 WL 1503429, at *8-10 (N.D. Cal. Apr. 1, 2015) (denying defendants' motion to dismiss plaintiff's UCL claim, holding that plaintiff stated a claim under both the unlawful and unfairness prongs of the statute by alleging that the defendant failed to adhere to the terms of its own Privacy Policy in violation of Cal. Bus. & Prof. Code § 22576, and plaintiff alleged that defendants' payment processing services were not free because they allegedly retained a portion of the $1.77 app price for each transaction); *see generally supra* § 26.13[6] (analyzing the duty to post a privacy policy imposed on companies that collect personal information from California residents). In *Svenson*, the plaintiff pled around *In re Facebook Privacy Litig.*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal with prejudice of plaintiffs' UCL claim where plaintiffs could not allege that they "lost money or property as a result of the unfair competition.") by alleging the existence of a contract and a fee that does not appear to have been plausible in light of the actual written contract entered into by the plaintiff and defendants.

[177]*See, e.g.*, *Campbell v. Facebook, Inc.*, 77 F. Supp. 3d 836, 849 (N.D. Cal. 2014); *Opperman v. Path, Inc.*, 87 F. Supp. 3d 1018, 1056 n.22 (N.D. Cal. 2014); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715 (N.D. Cal. 2011); *Claridge v. RockYou, Inc.*, 785 F. Supp. 2d 855, 862 (N.D. Cal. 2011).

[178]*See, e.g.*, *Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 35-36 (2d Cir. 2017), *aff'g*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *10-13 (S.D.N.Y. Aug. 17, 2016) (affirming dismissal of plaintiffs' claims under N.Y. Gen. Bus. L. § 349 for failure to allege facts showing that they had suffered an injury cognizable under that section, in a putative class action suit based on defendants' alleged use of tracking cookies, because "§ 349 injury has been recognized only where confidential, individually identifiable information—such as medical records or a Social Security number—is collected without the individual's knowledge or consent."); *Cohen v. Casper Sleep Inc.*, Nos. 17cv9325, 17cv9389, 17cv9391, 2018 WL 3392877, at *7-9 (S.D.N.Y. July 12, 2018) (dismissing plaintiff's claim against NaviStone, a

Statutory violations framed as unfair competition claims will suffer a similar fate. For example, claims for alleged statutory privacy violations—such as a failure to provide notice of the right to request information—and unfair competition claims premised on that alleged failure, may be dismissed where no real injury can be pled.[179] False advertising claims under California law[180] likewise will be dismissed

---

marketing company and data broker that offered code to e-commerce vendors to help them identify who visited their websites by scanning visitors' computers for information that could be used for de-anonymization, for failing to satisfy the injury requirement of section 349); *Tyler v. Michaels Stores, Inc.*, 840 F. Supp. 2d 438, 448–51 (D. Mass. 2012) (dismissing a claim under Massachusetts' unfair trade practices statute, Mass. Gen. Laws ch. 93A, § 2 because receiving unwanted mail and other alleged injuries stemming from the defendant's alleged disclosure of her zip code information was not an injury cognizable under chapter 93A); *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *5–6 (W.D. Wash. Dec. 1, 2011) (dismissing with leave to amend an unfair competition claim in a putative class action suit over the alleged use of browser and flash cookies because Washington's Consumer Protection Act requires "a specific showing of injury").

[179]*See, e.g.*, *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 996 F. Supp. 2d 942, 1009-10 (S.D. Cal. 2014) (dismissing plaintiffs' section 1789.84(b) claim for economic damages, but allowing plaintiffs to pursue their injunctive relief claims under section 1798.84(e)); *Murray v. Time Inc.*, No. C 12-00431 JSW, 2012 WL 3634387 (N.D. Cal. Aug. 24, 2012) (dismissing, with leave to amend, plaintiff's claims under Cal Civil Code § 1798.83 and Cal. Bus. & Professions Code § 17200 for lack of statutory standing due to lack injury and dismissing plaintiff's claim for injunctive relief for lack of Article III standing; rejecting arguments that plaintiffs had experienced economic or informational injury); *Boorstein v. Men's Journal LLC,* No. CV 12-771 DSF (Ex), 2012 WL 3791701 (C.D. Cal. Aug. 17, 2012) (dismissing with prejudice plaintiff's claims under Cal Civil Code § 1798.83 and Cal. Bus. & Professions Code § 17200 for lack of statutory standing due to lack injury; rejecting arguments that plaintiffs had experienced economic or informational injury); *King v. Condé Nast Publications,* No. CV-12-0719-GHK (Ex), 2012 WL 3186578 (C.D. Cal. Aug. 3, 2012) (dismissing the same claims on the same grounds, with leave to amend); *Miller v. Hearst Communications, Inc.,* No. CV 12-0733-GHK (PLAx), 2012 WL 3205241 (C.D. Cal. Aug. 3, 2012) (dismissing the same claims, on the same grounds, with leave to amend); *Boorstein v. Men's Journal LLC,* No. CV 12-771 DSF (Ex), 2012 WL 2152815 (C.D. Cal. June 14, 2012) (dismissing the same claims on the same grounds, with leave to amend); *see generally supra* § 26.13[6][D] (analyzing section 1798.83).

[180]Cal. Bus. & Prof. Code §§ 17500, *et seq.* California's false advertising law reaches advertising that is false as well as advertising that, although true, is either actually misleading or has "a capacity, likelihood or tendency to deceive or confuse the public." *Low v. LinkedIn Corp.*, 900 F.

where a plaintiff cannot show that it has suffered injury in fact and lost money or property.[181]

Similarly, a claim under California's Computer Crime law (also known as the California Comprehensive Computer Data Access and Fraud Act)[182] is only actionable where a plaintiff can show "damage or loss."[183] A CCCDAFA claim also may be unavailable absent circumvention; merely accessing information may not be enough.[184]

Supp. 2d 1010, 1026 (N.D. Cal. 2012), *quoting Leoni v. State Bar*, 39 Cal. 3d 609, 626, 217 Cal. Rptr. 423 (1985).

[181]*See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1026-27 (N.D. Cal. 2012) (dismissing with prejudice Low's false advertising claim because personal information does not constitute money or property and dismissing with prejudice both his claim and that of plaintiff Masand, who paid $24.99 for a "Job Seeker Platinum" LinkedIn subscription and therefore met the threshold requirement of showing a loss of money or property, where neither could allege reliance on the allegedly false advertisements or misrepresentations).

[182]Cal. Penal Code § 502. A claim under section 502 is similar to a claim under the federal Computer Fraud & Abuse Act, 18 U.S.C.A. § 1030, except that "the California statute does not require *unauthorized* access. It merely requires *knowing* access." *U.S. v. Christensen*, 828 F.3d 763, 789 (9th Cir. 2016) (emphasis in original). *Access*, according to the Ninth Circuit, "includes logging into a database with a valid password and subsequently taking, copying, or using the information in the database improperly." *Id.*; *see also Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058, 1069 (9th Cir. 2016) (affirming liability under section 502 where the defendant continued to access Facebook's servers after having received a cease and desist letter instructing it to stop doing so). According to one court, a claim under section 502 may not be viable where the data accessed is publicly available. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 273 F. Supp. 3d 1099, 1115 n.13 (N.D. Cal. 2017).

[183]Cal. Penal Code § 502(e); *see also Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 152 (3d Cir. 2015) (affirming dismissal of plaintiffs' claim under section 502 where plaintiffs alleged loss of the value of personal data, which the Third Circuit held did not amount to damage or loss), *cert. denied*, 137 S. Ct. 36 (2016); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715–16 (N.D. Cal. 2011) (dismissing plaintiffs' section 502 claims, some with and some without prejudice), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim but reversing dismissal of their breach of contract and fraud claims; plaintiffs did not appeal the dismissal of their section 502 claim); *see generally infra* § 44.09 (analyzing section 502).

[184]*See, e.g., In re Google Android Consumer Privacy Litig.*, No. 11-2264, 2013 WL 1283236, at *11 (N.D. Cal. Mar. 26, 2013) ("Courts within this District have interpreted 'without permission' to require that a defendant access a network in a manner that circumvents technical or

Common law privacy claims may be difficult to assert in data privacy cases[185] absent an ability to characterize the alleged intrusion as highly offensive to a reasonable person.[186]

---

code based barriers in place to restrict or bar a user's access."; internal quotation marks omitted).

[185]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 294-95 (3d Cir. 2016) (affirming dismissal of plaintiffs' New Jersey intrusion upon seclusion claim against Google for allegedly using tracking cookies to track website activity by children because tracking cookies can serve legitimate commercial purposes and "Google used third-party cookies on Nick.com in the same way that it deploys cookies on myriad others websites. Its decision to do so here does not strike us as sufficiently offensive, standing alone, to survive a motion to dismiss."), *cert. denied*, 137 S. Ct. 624 (2017); *In re Facebook Internet Tracking Litigation*, 263 F. Supp. 3d 836, 846-47 (N.D. Cal. 2017) (dismissing claims for common law intrusion upon seclusion and invasion of privacy under the California Constitution because plaintiffs did not establish that they had a reasonable expectation of privacy in the URLs of the pages they visited; "Plaintiffs could have taken steps to keep their browsing histories private. For instance, as Facebook explained in its privacy policy, '[y]ou can remove or block cookies using the settings in your browser.' . . . Similarly, users can 'take simple steps to block data transmissions from their browsers to third parties,' such as 'using their browsers in 'incognito' mode' or 'install[ing] plugin browser enhancements.' . . . Facebook's intrusion could have been easily blocked, but Plaintiffs chose not to do so."); *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 933 n.5 (N.D. Cal. 2015) (dismissing intrusion upon seclusion claims in a putative data privacy class action suit because plaintiffs "could not have held a subjective expectation of privacy in their browsing histories that was objectively reasonable"); *In re Google, Inc. Privacy Policy Litigation*, 58 F. Supp. 3d 968, 987-88 (N.D. Cal. 2014) (dismissing with prejudice plaintiffs' intrusion upon seclusion claim based on plaintiffs' inability to meet the "high bar" to allege the requisite "intrusion [that is] highly offensive to a reasonable person"); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (finding unauthorized disclosure of mobile device information to not be an egregious breach of social norms); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (finding disclosure of LinkedIn data insufficiently offensive); *McConnell v. Georgia Department of Labor*, 345 Ga. App. 669, 680-82, 814 S.E.2d 790, 800-01 (2018) (affirming dismissal of plaintiff's invasion of privacy claim, where the Department of Labor had sent an email to approximately 1,000 Georgians who had applied for unemployment benefits, which included a spreadsheet that listed the name, social security number, home phone number, email address, and age of over 4,000 state residents, because there was no intrusion on plaintiff's seclusion); *see generally supra* §§ 12.02[3][B], 26.08 (analyzing tort of unreasonable intrusion on seclusion, at greater length).

[186]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 295 (3d Cir. 2016) (vacating an order dismissing plaintiffs' intrusion upon seclusion claim against Viacom based on the collection of information using allegedly duplicitous tactics, where the Nickelodeon website al-

Alleged data privacy violations also may be difficult to assert as common law privacy claims where information may have been exposed but it is not clear that it in fact was accessed. At least at common law, "[f]or a person's privacy to be invaded, their personal information must, at a minimum, be disclosed to a third party."[187]

---

legedly included the false message: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!"; "Viacom's message to parents about not collecting children's personal information may have created an expectation of privacy on Viacom's websites, it also may have encouraged parents to permit their children to browse those websites under false pretenses."), *cert. denied*, 137 S. Ct. 624 (2017); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 149-52 (3d Cir. 2015) (holding that plaintiffs stated claims under the California Constitution and California tort law where plaintiffs alleged practices that allegedly went beyond disclosed tracking to allegedly include overriding cookie blocking software to access information and involved alleged misstatements about its practices), *cert. denied*, 137 S. Ct. 36 (2016); *In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1231-33 (C.D. Cal. 2017) (denying defendants' motion to dismiss plaintiffs' intrusion upon seclusion claims under California, Florida and Washington law and invasion of privacy under the California Constitution and the Massachusetts Privacy Act where plaintiffs alleged that the interactivity function on Vizio Smart TVs remained on even when it had been turned off, resulting in the collection of information about plaintiffs' identities and television viewing histories); *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962, 991-93 (N.D. Cal. 2015) (denying defendants' motions to dismiss intrusion on seclusion claims arising from the transfer of contact information from users' mobile address books when users selected the "Find Friends" feature to connect with friends on social networks).

[187]*In re SAIC Corp.*, 45 F. Supp. 2d 14, 28 (D.D.C. 2014); *see also Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' invasion of privacy claims under the California Constitution and common law where plaintiffs alleged that the defendant disclosed to third parties their LinkedIn IDs and the URLs of the LinkedIn profile pages that the users viewed because "[a]lthough Plaintiffs postulate that these third parties could, through inferences, de-anonymize this data, it is not clear that anyone has actually done so."). In *SAIC*, Judge James E. Boasbert, Jr. explained that "[i]f no one has viewed your private information (or is about to view it imminently), then your privacy has not been violated." *Id.* at 28-29, *citing* 5 C.F.R. § 297.102 (Under Privacy Act, "[d]isclosure means providing *personal review* of a record, or a copy thereof, to someone other than the data subject or the data subject's authorized representative, parent, or legal guardian.") (emphasis added); *Walia v. Chertoff*, No. 06—6587, 2008 WL 5246014, at *11 (E.D.N.Y. Dec. 17, 2008) ("accessibility" is not the same as "active disclosure"); *Schmidt v. Dep't of Veterans Affairs*, 218 F.R.D. 619, 630 (E.D. Wis. 2003) (Disclosure is "the placing into the view of another information which was previously unknown," requiring that information be "actually viewed."); *Harper v.*

Some claims also suffer because of efforts to shoehorn novel privacy theories into existing unfair competition, statutory or common law remedies.[188] For example, in *Steinberg v. CVS Caremark Corp.*,[189] the court dismissed claims under the Pennsylvania Unfair Trade Practices and Consumer Protection Law and for unjust enrichment and invasion of privacy, in a putative class action brought by a union and its members, alleging that the defendant sold de-identified information obtained in connection with filling plaintiffs' prescriptions to third parties who plaintiffs alleged potentially could de-anonymize it. Plaintiffs had alleged that the defendants made material misrepresentations in their privacy statements, but the court found this practice to be consistent with CVS's privacy policy statement that defendants safeguarded information that "may identify" consumers, noting that the FTC's Privacy Rule promulgated under HIPAA[190] places no restrictions on the use of information once de-identified.[191] Plaintiffs' unfair competition and unjust enrichment claims were dismissed based on the lack of any

---

United States, 423 F. Supp. 192, 197 (D.S.C. 1976) (Disclose means "the imparting of information which in itself has meaning and which was previously unknown to the person to whom it was imparted."); *Fairfax Hospital v. Curtis*, 492 S.E.2d 642, 644 (Va. 1997) (violation where third party "possess[ed]" and "reviewed" records); *see also Storm v. Paytime, Inc.*, 90 F. Supp. 3d. 359, 368 (M.D. Pa. 2015) (dismissing Pennsylvania privacy claims of employees for lack of standing where no information had been disclosed to a third party after a cyber-attack on the defendant's payroll provider).

[188]*See, e.g.*, *McConnell v. Georgia Department of Labor*, 345 Ga. App. 669, 678, 680-82, 814 S.E.2d 790, 798, 800-01 (2018) (affirming dismissal because there was no general duty of care to safeguard personal information under Georgia law and none could be inferred from the enactment of Georgia's security breach notification statute or a statute prohibiting use and display of social security numbers, and because plaintiff could not state breach of fiduciary duty or invasion of privacy claims—where the Department of Labor had sent an email to approximately 1,000 state residents who had applied for unemployment benefits, which included a spreadsheet that listed the name, social security number, home phone number, email address, and age of over 4,000 state residents—because there was no confidential relationship to support a breach of fiduciary duty claim, and no intrusion on plaintiff's seclusion, to support a common law claim for invasion of privacy).

[189]*Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331 (E.D. Pa. 2012).

[190]45 C.F.R. §§ 160.103, 164.502(d)(1) to 164.502(d)(2); *supra* § 26.11.

[191]*See Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331, 336-38 (E.D. Pa. 2012).

value to the information, among other grounds.[192]

A claim for common law trespass generally requires a showing of substantial impairment, not merely unauthorized access.[193] For this reason, plaintiffs in putative behavioral advertising privacy class action suits may have difficulty stating a claim even where unauthorized access is alleged.[194]

Where a plaintiff cannot state a claim under ECPA because access was found to be authorized by a Privacy Policy, TOU or otherwise, the plaintiff also may have difficulty establishing a claim for common law invasion of

---

[192]*See Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331, 337-42 (E.D. Pa. 2012).

[193]*See, e.g.*, *Mount v. PulsePoint, Inc.*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *9-10 (S.D.N.Y. Aug. 17, 2016) (dismissing plaintiffs' trespass claim in a putative class action suit based on alleged use of tracking cookies), *aff'd on other grounds*, 684 F. App'x 32 (2d Cir. 2017); *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1347, 1 Cal. Rptr. 3d 32 (2003); *see generally supra* § 5.05[1] (analyzing computer trespass cases).

[194]*See, e.g.*, *In re Facebook Internet Tracking Litigation*, No. 5:12-md-02314-EJD, 2017 WL 2834113, at *3 (N.D. Cal. June 30, 2017) (dismissing plaintiff's claim of trespass to chattels for lack of standing); *In re Google Android Consumer Privacy Litig.,* No. 11-MD-02264, 2013 WL 1283236, at *13 (N.D. Cal. Mar. 26, 2013) (dismissing plaintiff's trespass to chattels claim because CPU processing, battery capacity, and Internet connectivity do not constitute a harm sufficient to establish a cause of action for trespass); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *15-16 (N.D. Cal. Mar. 26, 2013) (dismissing plaintiff's trespass claim with leave to amend where the plaintiff alleged that Pandora installed unwanted code that consumed portions of the memory on his mobile device); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1069 (N.D. Cal. 2012) (dismissing plaintiffs' trespass claims with prejudice where plaintiffs alleged that (1) the creation of location history files and app software components "consumed portions of the cache and/or gigabytes of memory on their devices" and (2) apps had taken up valuable bandwidth and storage space on mobile devices and the defendants' conduct subsequently shortened the battery life of the device; "While these allegations conceivably constitute a harm, they do not plausibly establish a significant reduction in service constituting an interference with the intended functioning of the system, which is necessary to establish a cause of action for trespass."); *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *6 (W.D. Wash. Dec. 1, 2011) (dismissing with leave to amend a putative class action claim for trespass under Washington law based on the alleged use of browser and flash cookies where plaintiffs "failed to plead any facts that would permit the Court to infer that they sustained any plausible harm to a materially valuable interest in the condition, quality, or value of their computers.").

privacy premised on the same unauthorized access.[195] Privacy claims arising at common law or created by the California Constitution likewise may not be viable in a data privacy or behavioral advertising case where the information allegedly disclosed is anonymized data such as social network profile IDs or the URLs viewed by users[196] or unique mobile device identifier numbers, personal data and geolocation information[197] (except in limited circumstances[198]).

---

[195]*See, e.g.*, *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (dismissing plaintiff's California common law privacy claim based on public disclosure of private facts and intrusion with leave to amend where the plaintiff alleged merely that he provided Pandora with PII, which it then disclosed to third parties; "Yunker does not allege that Pandora tracked his movements or obtained and then either disclosed or left unencrypted any type of sensitive financial information, medical information, or passwords."); *Deering v. CenturyTel, Inc.*, No. CV-10-63-BLG-RFC, 2011 WL 1842859 (D. Mont. May 16, 2011) (dismissing a putative class action alleging an ECPA violation and intrusion upon seclusion under Montana law where defendant's privacy policy and an email sent to subscribers advising them that the Policy had been updated, notified subscribers that CenturyTel, an ISP, used cookies and web beacons to gather information on its subscribers' browsing history, which it shared with NebuAd, a provider of tailored advertising services); *Mortensen v. Bresnan Communication, LLC*, No. CV 10-13-BLG-RFC, 2010 WL 5140454 (D. Mont. Dec. 13, 2010) (dismissing plaintiff's invasion of privacy claim where the complaint sufficiently alleged plaintiff's subjective expectation of seclusion or solitude but this subjective expectation was not objectively reasonable in light of the disclosures in defendant's Subscriber Agreement and Privacy Notice and notice that use of the defendant's service constituted acceptance of the terms of the Subscriber Agreement and Privacy Notice; also dismissing plaintiff's ECPA claim, but denying defendant's motion with respect to trespass and CFAA claims), *vacated on other grounds*, 722 F.3d 1151, 1157-61 (9th Cir. 2013) (holding that the lower court erred in declining to compel arbitration). In the words of the *Deering* court, "there is no [objectively] reasonable expectation of privacy when a plaintiff has been notified that his Internet activity may be forwarded to a third party to target him with advertisements." *Deering v. CenturyTel, Inc.,* No. CV-10-63-BLG-RFC, 2011 WL 1842859, at *2 (D. Mont. May 16, 2011).

[196]*See, e.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' invasion of privacy claims under the California Constitution and common law where plaintiffs alleged that the defendant disclosed to third parties their LinkedIn IDs and the URLs of the LinkedIn profile pages that the users viewed because "[a]lthough Plaintiffs postulate that these third parties could, through inferences, de-anonymize this data, it is not clear that anyone has actually done so.").

[197]*See In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 294-95 (3d Cir. 2016) (affirming dismissal of plaintiffs' New Jersey intru-

A plaintiff may be unable to state a claim for unjust enrich-

---

sion upon seclusion claim against Google for allegedly using tracking cookies to track website activity by children because tracking cookies can serve legitimate commercial purposes and "Google used third-party cookies on Nick.com in the same way that it deploys cookies on myriad others websites. Its decision to do so here does not strike us as sufficiently offensive, standing alone, to survive a motion to dismiss."), *cert. denied*, 137 S. Ct. 624 (2017); *In re Facebook Internet Tracking Litig.*, 140 F. Supp. 3d 922, 933 n.5 (N.D. Cal. 2015) (dismissing intrusion upon seclusion claims in a putative data privacy class action suit because plaintiffs "could not have held a subjective expectation of privacy in their browsing histories that was objectively reasonable" because 'Internet users have no expectation of privacy in the . . . IP addresses of the websites they visit . . . [and] should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.' "; citing *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007)); *In re Google, Inc. Privacy Policy Litigation*, 58 F. Supp. 3d 968, 987-88 (N.D. Cal. 2014) (dismissing with prejudice plaintiffs' intrusion upon seclusion claim based on plaintiffs' inability to meet the "high bar" to allege the requisite "intrusion [that is] highly offensive to a reasonable person"); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (holding that the alleged disclosure to third parties of the unique device identifier numbers of Apple mobile devices, personal data stored by users on those devices and geolocation information did not involve an egregious breach of social norms and therefore was not actionable under California's constitutional right to privacy); *see also In re Google Android Consumer Privacy Litig.,* No. 11-MD-02264, 2013 WL 1283236, at *10 (N.D. Cal. Mar. 26, 2013) (following *iPhone Application Litigation* in dismissing plaintiff's constitutional right to privacy claim where plaintiffs alleged that Google allowed third party affiliates such as AdMob and AdWhirl to obtain unencrypted user data); *Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *14-15 (N.D. Cal. Mar. 26, 2013) (following *iPhone Application Litigation* in dismissing plaintiff's claim with leave to amend where the plaintiff merely alleged that Pandora obtained his PII and provided it to advertising libraries for marketing purposes, allegedly in violation of Pandora's privacy policy).

[198]*See, e.g.*, *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262, 295 (3d Cir. 2016) (vacating an order dismissing plaintiffs' intrusion upon seclusion claim against Viacom based on the collection of information using allegedly duplicitous tactics, where the Nickelodeon website allegedly included the false message: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!"; "Viacom's message to parents about not collecting children's personal information may have created an expectation of privacy on Viacom's websites, it also may have encouraged parents to permit their children to browse those websites under false pretenses."), *cert. denied*, 137 S. Ct. 624 (2017); *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 149-52 (3d Cir. 2015) (holding that plaintiffs stated claims under the California Constitution and California tort law where plaintiffs alleged practices that allegedly went beyond disclosed tracking to allegedly include overriding cookie blocking software

ment, which is a quasi-contract claim, where he or she entered into an express agreement, such as Terms of Use or a Privacy Policy, explicitly permitting the collection, use or dissemination of personal information.[199] A state law conversion claim may suffer the same defect.[200] Conversion claims similarly may fail if user contact information is not viewed as property under applicable state law or if the data at issue is generated by the Internet site or service, rather than the consumer.[201]

---

to access information and involved alleged misstatements about its practices) *cert. denied*, 137 S. Ct. 36 (2016); *Opperman v. Path, Inc.*, 84 F. Supp. 3d 962 (N.D. Cal. 2015) (dismissing conversion and injunctive relief claims but denying defendants' motions to dismiss intrusion on seclusion claims arising from the transfer of contact information from users' mobile address books when users selected the "Find Friends" feature to connect with friends on social networks).

[199]*See, e.g.*, *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *6 (W.D. Wash. Dec. 1, 2011) (dismissing with leave to amend a putative class action suit over the alleged use of browser and flash cookies where the defendant's potential use of browser and flash cookies was disclosed to users in the defendant's "Conditions of Use and Privacy Notice" so therefore any use was not inequitable and because "Plaintiffs have not plead any facts from which the Court might infer that Defendant's decision to record, collect, and use its account of Plaintiffs' interactions with Defendant came at Plaintiffs' expense."); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 718 (N.D. Cal. 2011) (dismissing plaintiffs' unjust enrichment claim with prejudice where plaintiffs assented to Facebook's "Terms and Conditions and Privacy Policy"), *aff'd in part, rev'd in part, on other grounds*, 572 F. App'x 494 (9th Cir. 2014) (affirming dismissal of plaintiffs' UCL claim but reversing dismissal of their breach of contract and fraud claims; plaintiffs did not appeal the dismissal of their unjust enrichment claim).

[200]*See, e.g.*, *In re Sony Gaming Networks and Customer Data Security Breach Litigation*, 903 F. Supp. 2d 942, 974 (S.D. Cal. 2012) (dismissing with prejudice plaintiffs' claims for conversion because personal information could not be construed as property that was somehow "delivered" to Sony and expected to be returned, and because the information was stolen as a result of a criminal intrusion of Sony's Network); *AD Rendon Communications, Inc. v. Lumina Americas, Inc.*, No. 04-CV-8832 (KMK), 2007 WL 2962591 (S.D.N.Y. Oct. 10, 2007) ("[E]ven if a plaintiff meets all of the elements of a conversion claim, the claim will still be dismissed if it is duplicative of a breach of contract claim."), *citing Wechsler v. Hunt Health Systems, Ltd.*, 330 F. Supp. 2d 383, 431 (S.D.N.Y. 2004) *and Richbell Information Services, Inc. v. Jupiter Partners, L.P.*, 309 A.D.2d 288, 765 N.Y.S.2d 575, 590 (1st Dep't 2003); *see generally supra* § 5.05[2] (analyzing conversion claims in connection with database protection and screen scraping).

[201]*See, e.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1030-31

Although not analyzed to date in a data privacy case, conversion claims also may not be viable under some state's laws because data privacy cases usually involve sharing personal information, not dispossession, but most states require a showing of dispossession (or at least substantial interference).[202]

Courts also have been skeptical that a legally cognizable benefit has been conferred when an unjust enrichment claim is premised on the alleged use of a user's browsing information[203] or zip code data[204] or the sale of de-identified personal

---

(N.D. Cal. 2012) (dismissing with prejudice plaintiffs' claim for conversion because personal information does not constitute property under California law, plaintiffs could not establish damages and some of the information allegedly "converted," such as a LinkedIn user ID number, was generated by LinkedIn, and therefore not property over which a plaintiff could claim exclusivity); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1074–75 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' conversion claim because personal information does not constitute property under California law, plaintiffs failed to establish that "the broad category of information referred to as 'personal information' is an interest capable of precise definition" and the court could not conceive how "the broad category of information referred to as 'personal information' . . . is capable of exclusive possession or control."); *see also Yunker v. Pandora Media, Inc.,* No. 11-CV-03113 JSW, 2013 WL 1282980, at *16-17 (N.D. Cal. Mar. 26, 2013) (following *iPhone Application Litigation* in dismissing plaintiff's conversion claim based on Pandora's alleged use of his PII with leave to amend); *see generally supra* §§ 5.05[2] (analyzing the law of conversion), 7.21 (intangible property and the law of conversion, addressed in the context of domain name registrations).

[202]*See, e.g.*, *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393, 437–38 (2d Cir. 2004) ("Traditionally, courts have drawn a distinction between interference by dispossession, . . . which does not require a showing of actual damages, . . . and interference by unauthorized use or intermeddling, . . . which requires a showing of actual damages . . . ."; citations omitted) (New York law); *eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1067 (N.D. Cal. 2000) (distinguishing trespass from conversion); *see generally supra* § 5.05[2] (analyzing the law of conversion); *see generally supra* § 5.05[2].

[203]*See, e.g.*, *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *6 (W.D. Wash. Dec. 1, 2011) (dismissing with leave to amend a putative class action suit over the alleged use of browser and flash cookies where the court held that the plaintiffs had failed to allege any legally cognizable benefit). Under Washington law, to establish unjust enrichment, a plaintiff must show that: (1) one party conferred a benefit on the other; (2) the party receiving the benefit had knowledge of that benefit; and (3) the party receiving the benefit accepted or retained the benefit under circumstances that would make it inequitable for the receiving party to retain it without paying for its value. *See id., quoting Cox v.*

information.[205]

Under California law, a separate claim may not be asserted for unjust enrichment, which since 2011 courts have characterized as a request for restitution, not a separate cause of action under California law.[206] Other states, such as Illinois[207] and New Jersey,[208] similarly do not recognize unjust enrichment as a separate cause of action. Even where

---

O'Brien, 150 Wash. App. 24, 37, 206 P.3d 682 (2009). "The crux of an unjust enrichment claim is 'that a person who is unjustly enriched at the expense of another is liable in restitution to the other.' " *Del Vecchio v. Amazon.com, Inc.,* No. C11-366-RSL, 2011 WL 6325910, at *6 (W.D. Wash. Dec. 1, 2011), *quoting Dragt v. Dragt/DeTray, LLC*, 139 Wash. App. 560, 576, 161 P.3d 473 (2007).

[204]*See Tyler v. Michaels Stores, Inc.*, 840 F. Supp. 2d 438, 451–52 (D. Mass. 2012) (dismissing plaintiff's unjust enrichment claim under Massachusetts law where the plaintiff had not alleged that Michaels ever paid for zip codes or that reasonable people would expect payment for revealing a zip code in connection with a routine retail transaction); *see also Karp v. Gap, Inc.*, No. 13–11600–GAO, 2014 WL 4924229, at *2 (D. Mass. Sept. 29, 2014) (dismissing unjust enrichment claim arising out of the merchant's collection of zip codes); *Lewis v. Collective Brands, Inc.*, No. 13–12702–GAO, 2014 WL 4924413, at *1-2 (D. Mass. Sept. 29, 2014) (dismissing unjust enrichment claim arising out of a merchant's collection of zip codes).

[205]*See Steinberg v. CVS Caremark Corp.*, 899 F. Supp. 2d 331, 342 (E.D. Pa. 2012) (dismissing plaintiffs' claim for unjust enrichment under Pennsylvania law, in a putative class action suit, where plaintiffs had no reasonable expectation that they would be compensated for disclosing information for the purpose of having their prescriptions filled).

[206]*See Hill v. Roll Int'l Corp.*, 195 Cal. App. 4th 1295, 1307, 128 Cal. Rptr. 3d 109 (2011) (holding that "[u]njust enrichment is not a cause of action, just a restitution claim."); *see also, e.g., Astiana v. Hain Celestial Group, Inc.*, 783 F.3d 753, 762 (9th Cir. 2015) (explaining that in California, there is no standalone cause of action for unjust enrichment, which is synonymous with restitution); *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1031 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' claim for unjust enrichment because such a claim is not viable under California law); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1075–76 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' claim for unjust enrichment based on *Hill v. Roll Int'l Corp.*); *Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 814–15 (N.D. Cal. 2011) (dismissing a claim for unjust enrichment in light of Hill v. Roll Int'l Corp., "[n]otwithstanding earlier cases suggesting the existence of a separate, stand-alone cause of action for unjust enrichment . . . ."); *In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963, at *15 (N.D. Cal. Sept. 20, 2011) (dismissing plaintiff's claim for unjust enrichment, finding there is no longer any such cognizable claim under California law).

[207]*See Sheridan v. iHeartMedia, Inc.*, 255 F. Supp. 3d 767, 781 (N.D. Ill. June 5, 2017) (dismissing plaintiffs' unjust enrichment claim, holding

recognized, a claim for unjust enrichment may not be viable if the data does not have a value or enrich the defendant.[209]

California likewise does not recognize a separate cause of action for restitution, which is a remedy that a plaintiff may elect, not a claim.[210]

Even negligence claims may be difficult to sustain in the absence of economic injury.[211] Negligence generally requires

---

that unjust enrichment is not an independent cause of action), *citing Gagnon v. Schickel*, 368 Ill. Dec. 240, 983 N.E.2d 1044, 1052 (2012).

[208]*See In re Nickelodeon Consumer Privacy Litigation*, Case Nos. Civ. A. 12-07829, Civ. A. 13-03729, Civ. A. 13-03731, Civ. A. 13-03755, Civ. A. 13-03756, Civ. A. 13-03757, 2014 WL 3012873, at *19 (D.N.J. July 2, 2014) (dismissing with prejudice plaintiffs' common law unjust enrichment claim in a data privacy case), *aff'd in part, rev'd in part, on other grounds*, 827 F.3d 262, 271 n.36 (3d Cir. 2016) (noting, in connection with affirming the district court's dismissal of plaintiffs' New Jersey Computer Related Offenses Act claim, that the district court dismissed plaintiffs' common law unjust enrichment "claim with prejudice. . . . The plaintiffs eventually explained [on appeal] that they sought to use unjust enrichment 'not as an independent action in tort, but as a measure of damages under the [New Jersey Computer Related Offenses Act] in a quasi-contractual sense."), *cert. denied*, 137 S. Ct. 624 (2017).

[209]*See, e.g.*, *Mount v. PulsePoint, Inc.*, 684 F. App'x 32, 36-37 (2d Cir. 2017), *aff'g*, 13 Civ. 6592 (NRB), 2016 WL 5080131, at *13 (S.D.N.Y. Aug. 17, 2016) (affirming dismissal of plaintiffs' claim where they failed to plead injury based on misappropriation of the value of their browsing information). *But see Moeller v. American Media, Inc.*, 235 F. Supp. 3d 868, 875-76 (E.D. Mich. 2017) (holding that plaintiff stated a claim for unjust enrichment under Michigan law, which requires a plaintiff to allege (1) the receipt of a benefit by the defendant from the plaintiff and (2) an inequity resulting to the plaintiff because of the retention of that benefit, where plaintiff alleged that defendants' allegedly unlawful disclosure of plaintiffs' personal information rendered their magazine subscriptions from defendants less valuable and that the defendants retained this benefit); *see also Perlin v. Time, Inc.*, 237 F. Supp. 3d 623, 643 (E.D. Mich. 2017) (holding that plaintiff stated a plausible unjust enrichment claim by alleging that she conferred a benefit on defendant by paying subscription fees and providing personal information, which the defendant allegedly monetized by selling to "data miners" including information allegedly prohibited from disclosure by Michigan's Preservation of Personal Privacy Act, and that the defendant retained this benefit); *Raden v. Martha Stewart Living Omnimedia, Inc.*, Case No. 16-12808, 2017 WL 3085371, at *4 (E.D. Mich. July 20, 2017) (following *Moeller* and *Perlin*).

[210]*In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1076 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' claim for unjust enrichment, assumpsit and restitution).

[211]*See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1031-32 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' claim); *In re iPhone*

a showing of (1) a legal duty to use due care, (2) a breach of that duty, (3) injury and (4) proximate causation (that the breach was the proximate or legal cause of injury).[212] To state a claim, a plaintiff in a data privacy case generally must show an "appreciable, nonspeculative, present injury."[213] Further, in most states, purely economic losses generally are not recoverable as tort damages.[214] A negligence claim also may

---

Application Litig., Case No. 11-MD-02250-LHK, 2011 WL 4403963, at *9 (N.D. Cal. Sept. 20, 2011) (dismissing plaintiffs' claim with leave to amend); *see also infra* § 27.07 (analyzing the extensive body of negligence case law in data security breach putative class action suits).

[212]*E.g.*, *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1031-32 (N.D. Cal. 2012); *In re iPhone Application Litig.,* Case No. 11-MD-02250-LHK, 2011 WL 4403963, at *9 (N.D. Cal. Sept. 20, 2011).

[213]*Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1032 (N.D. Cal. 2012); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1064 (N.D. Cal. 2012); *see also Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 913–14 (N.D. Cal. 2009) (granting summary judgment for the defendant on plaintiff's negligence claim in a security breach case brought by a job applicant whose personal information had been stored on a laptop of the defendant's that had been stolen, because the risk of future identity theft did not rise to the level of harm necessary to support plaintiff's negligence claim, which under California law must be appreciable, non-speculative, and present), *aff'd mem.*, 380 F. App'x 689 (9th Cir. 2010); *Pinero v. Jackson Hewitt Tax Service Inc.*, 594 F. Supp. 2d 710 (E.D. La. 2009) (holding that the mere possibility that personal information was at increased risk did not constitute an actual injury sufficient to state claims for fraud, breach of contract (based on emotional harm), negligence, among other claims, but holding that the plaintiff had stated a claim for invasion of privacy).

[214]*See, e.g.*, *In re TJX Cos. Retail Security Breach Litig.*, 564 F.3d 489, 499–500 (1st Cir. 2009) (affirming, in a security breach case arising out of a hacker attack, dismissal of plaintiffs' negligence claim based on the economic loss doctrine (which holds that purely economic losses are unrecoverable in tort and strict liability actions in the absence of personal injury or property damage)); *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 533 F.3d 162, 175–76 (3d Cir. 2008) (dismissing issuer bank's negligence claim against a merchant bank for loss resulting from a security breach based on the economic loss doctrine, which provides that no cause of action exists for negligence that results solely in economic damages unaccompanied by physical or property damage); *In re Target Corp. Data Security Breach Litigation*, 66 F. Supp. 3d 1154, 1171-76 (D. Minn. 2014) (dismissing plaintiffs' California, Illinois and Massachusetts negligence claims under the economic loss rule in data security breach putative class action suit); *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1064 (N.D. Cal. 2012) (dismissing with prejudice plaintiffs' negligence claim in a data privacy putative class action suit, holding that under California law injuries from disappointed expectations from a commercial transaction must be addressed through contract, not tort law); *In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518, 528–31 (N.D. Ill. 2011) (dismiss-

be difficult to sustain where a privacy policy discloses that information will be shared, undermining any argument that there was a duty to keep it confidential.

In some cases involving the use of mobile devices, plaintiffs have alleged breach of the implied warranty of merchantability, which may fail because any alleged privacy violation does not necessarily mean that the device is not "fit for the ordinary purposes" for which the goods were intended.[215]

Intentional or negligent misrepresentation and fraud claims likewise need to be pled with specificity.[216]

Class Certification

Even if some Internet privacy claims can survive motions to dismiss or summary judgment, they are often ill-suited for class certification because the proposed classes are defined in terms of conduct for which no records exist, and are

---

ing plaintiffs' negligence and negligence *per se* claims under the economic loss rule in a security breach putative class action suit).

[215]*See, e.g.*, *In re iPhone 4S Consumer Litig.*, No. C 12-1127 CW, 2013 WL 3829653, at *15-16 (N.D. Cal. July 23, 2013) (holding that the implied warranty of merchantability is limited to "functions like making and receiving calls, sending and receiving text messages, or allowing for the use of mobile applications."; citing Cal. Civ. Code § 1791.1(a); Cal. Com. Code § 2134(2)(c)); *see also Birdsong v. Apple, Inc.*, 590 F.3d 955, 958 (9th Cir. 2009) (dismissing California implied warranty claim because the allegation that iPods were capable of operating at volumes that could damage users' hearing did not constitute an allegation that the product lacked "even the most basic degree of fitness" for the ordinary purpose of listening to music); *Williamson v. Apple, Inc.*, No. 5:11-cv-00377 EJD, 2012 WL 3835104, at *8 (N.D. Cal. Sept. 4, 2012) (dismissing implied warranty claim based on plaintiff's allegation that his iPhone 4's glass housing was defective because plaintiff did not allege his phone was deficient in making and receiving calls, sending and receiving text messages or allowing for the use of mobile applications). *But see In re: Carrier IQ, Inc. Consumer Litig.*, 78 F. Supp. 3d 1051, 1108-11 (N.D. Cal. 2015) (allowing breach of implied warranty claims to proceed under the laws of several states where plaintiffs alleged that software was included on mobile devices that collected and transmitted personal information provided adequate grounds under the laws of some states to allege that the devices were unmerchantable).

[216]*See, e.g., In re Vizio, Inc. Consumer Privacy Litig.*, 238 F. Supp. 3d 1204, 1228-34 (C.D. Cal. 2017) (dismissing (with leave to amend) plaintiffs' claims for fraud, negligent misrepresentation, and false advertising, but denying defendants' motion to dismiss plaintiffs' fraudulent omission, invasion of privacy and unjust enrichment claims, in a putative data privacy class action suit involving Vizio smart TVs).

therefore unascertainable,[217] or involve numerous individualized inquiries[218] into issues of consent, causation, reliance, and injury that may be specific to individual claimants and therefore potentially ill suited for class adjudication. For example, in *Murray v. Financial Visions, Inc.*,[219] the court denied class certification in a case alleging that the defendants, including a web hosting and email services company, violated plaintiff's privacy by intercepting and forwarding emails to comply with broker-dealer regulations, because demonstrating liability would have required numerous individualized inquiries, including whether the plaintiff had a reasonable expectation of privacy in each email, whether the email contained private information, and whether defendant's conduct caused any harm. Class certification also may be inappropriate where plaintiffs seek certification of a nationwide class based on state consumer protection laws.[220]

Similarly, in *In re Google Inc. Gmail Litigation*,[221] the court declined to certify a class action suit where common questions did not predominate because of the variety of different privacy policies and disclosures made to class members and the need for individualized proof of whether class members

---

[217]*See, e.g.*, *Messner v. Northshore University HealthSystem*, 669 F.3d 802, 825 (7th Cir. 2012) (holding that a class whose membership is defined by liability is improper).

[218]*See, e.g., Backhaut v. Apple Inc.*, Case No. 14–CV–02285–LHK, 2015 WL 4776427 (N.D. Cal. Aug. 13, 2015) (denying certification of a proposed class alleging that Apple wrongfully intercepted, stored, and otherwise prevented former Apple device users from receiving text messages sent to them from current Apple device users as unascertainable and one in which individualized issues would predominate over common questions, after concluding that plaintiffs lacked Article III standing to sue for injunctive relief and therefore were limited to damages on their claims under the Wiretap Act and California law).

[219]*Murray v. Financial Visions, Inc.*, No. CV-07-2578-PHX-FJM, 2008 WL 4850328 (D. Ariz. Nov. 7, 2008).

[220]*See, e.g.*, *Mazza v. American Honda Motor Co.*, 666 F.3d 581 (9th Cir. 2012) (holding that common questions did not predominate for purposes of class certification where a nationwide state law consumer class was sought given material differences between California and other state consumer protection laws).

[221]*In re Google Inc. Gmail Litigation*, Case No. 13-MD-02430-LHK, 2014 WL 1102660 (N.D. Cal. Mar. 18, 2014) (denying plaintiff's motion for class certification in consolidated privacy cases alleging violations of state and federal antiwiretapping laws in connection with the operation of Gmail).

provided consent.

In some cases, the claims remaining after motion practice are so limited that the named representative's claims are not typical of the class he or she seeks to represent and the named representative therefore is not an adequate representative. In *Svenson v. Google Inc.*,[222] for example, after several rounds of briefing motions to dismiss, class discovery and Google's motion for summary judgment, the court granted Google summary judgment on the remaining three claims for breach of contract, breach of the duty of good faith and fair dealing and unfair competition under Cal. Bus. & Prof. Code § 17200.[223] In the alternative, the court denied class certification because Svenson was subject to a unique defense to the contract claims, in that she asserted injury resulting from her lost expectation of privacy protection, but she purchased the "SMS MMS to Email" App at issue in the case for a second time on Google Play *after* discovering Google's alleged practice of granting sellers potential access to buyers' information and *after* filing the lawsuit. Accordingly, Judge Beth Labson Freeman ruled that, under those circumstances, the court would deny Svenson's motion for class certification for failure to establish typicality and adequacy of representation within the meaning of Federal Rule of Civil Procedure 23(a), even if it had not granted summary judgment in favor of Google.[224]

Whether putative plaintiffs can establish Article III standing to assert common claims also may impact class determinations.[225]

Class certification also may be improper where enforcement of a Privacy Statement under multiple different state

---

[222]*Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301 (N.D. Cal Dec. 21, 2016).

[223]*Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301, at *8-17 (N.D. Cal Dec. 21, 2016).

[224]*Svenson v. Google Inc.*, No. 13-cv-04080-BLF, 2016 WL 8943301, at *17 (N.D. Cal Dec. 21, 2016).

[225]*See, e.g., Gonzalez v. Corning,* 885 F.3d 186, 193-95 (3d Cir. 2018) (affirming denial of class certification where the plaintiffs could not establish commonality under Rule 23(a) because they lacked Article III standing to assert the one issue common to the putative class which was in the nature of an advisory opinion and therefore nonjusticiable); *see generally supra* § 25.07 (internet class actions).

laws would undermine a finding of commonality.[226]

On the other hand, in *Harris v. comScore,*[227] a court certified a class in a suit alleging Stored Communications Act and Computer Fraud and Abuse Act violations arising out of comScore's alleged practice of tracking the browsing activities of users who downloaded its tracking software. Likewise, claims under the Illinois Biometric Privacy Act have been certified as a class action.[228]

Courts also may certify equitable classes pursuant to Rule 23(b)(2) even where a common question class action would be inappropriate.[229]

While suits seeking to frame uses of new technologies as computer crime violations on the whole have not been very successful on the merits, potential claims may be easier to plead where a plaintiff can show a real injury and a clear lack of consent or authorization. For example, a court may allow a claim to proceed where a defendant is alleged to have engaged in conduct materially different from what was represented.[230] A violation of a privacy policy, for instance, is potentially actionable, but only if material and typically only if a plaintiff can show actual injury or damage, as well as

---

[226]*See Dolmage v. Combined Insurance Company of America*, 2017 WL 1754772, at *5-8 (N.D. Ill. May 3, 2013) (denying class certification in a breach of contract action based on an alleged breach of the defendant's privacy policy for allegedly failing to maintain adequate security, due to lack of commonality, where the issues of incorporation of the Privacy Policy by reference in the defendant's insurance contracts with putative class members and damages raised mixed factual and legal issues under the laws of multiple states).

[227]*Harris v. comScore*, 292 F.R.D. 579 (N.D. Ill. 2013).

[228]*In re Facebook Biometric Information Privacy Litig.*, __ F.R.D. __, 2018 WL 1794295, at *7-8 (N.D. Cal. 2018) (certifying a 23(b)(3) common question class of Illinois users of Facebook's website for whom the website created and stored a face template after June 7, 2011).

[229]*See, e.g.*, *Campbell v. Facebook Inc.*, 315 F.R.D. 250 (N.D. Cal. 2016) (denying plaintiffs' motion to certify a common question Rule 23(b)(3) class but certifying a Rule 23(b)(2) equitable class involving the alleged scanning of Facebook messages).

[230]*See, e.g.*, *Pinero v. Jackson Hewitt Tax Service Inc.*, 638 F. Supp. 2d 632 (E.D. La. 2009) (declining to dismiss plaintiff's fraud claim in a putative class action suit where plaintiff alleged that defendants' representation that they maintained privacy policies and procedures was false because at the time they made the statements defendants had not yet adopted policies to protect customer information).

standing to sue for a privacy policy violation.[231]

Likewise, where there is a security breach and resulting harm, a plaintiff may be able to state a claim.[232]

State law claims also may be framed as class action suits to try to force settlements, whether or not meritorious. For example, more than 150 class action suits were filed alleging violations of California's Song-Beverly Credit Card Act in the first six months of 2011 following the California Supreme Court's ruling earlier that year that collection of a person's zip code, without more, in connection with a credit card transaction, could constitute a privacy violation under California law.[233] The Act provides for statutory damages in cases where violations may be shown.

---

[231]Not all privacy policies will support breach of contract claims. *See, e.g.*, *Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196 (D.N.D. 2004) (holding that plaintiffs could not sue Northwest Airlines for breach of its privacy statement because the privacy policy did not give rise to a contract claim and they acknowledged that they had not read it). Even where actionable, a privacy policy may insulate a company from liability, rather than create exposure, if the practice at issue was adequately disclosed. *See, e.g.*, *Carlsen v. GameStop, Inc.*, 833 F.3d 903, 910-12 (8th Cir. 2016) (affirming dismissal of plaintiff's claims for breach of contract and alleged violations of Minnesota's Consumer Fraud Act, where GameStop's Privacy Policy, which was incorporated in its Terms of Service, did not define PII to include plaintiff's Facebook ID and browser history, which were the data elements that plaintiff alleged had been improperly shared); *Johnson v. Microsoft Corp.*, No. C06–0900RAJ, 2009 WL 1794400 (W.D. Wash. June 23, 2009); *see generally supra* § 26.14 (analyzing privacy statements and how to draft them).

In *Johnson*, the court granted partial summary judgment for Microsoft on plaintiffs' breach of contract claim in a putative class action suit where plaintiffs had alleged that Microsoft breached its End User License Agreement (EULA), which prohibited Microsoft from transmitting "personally identifiable information" from the user's computer to Microsoft, by collecting IP addresses. The court held that the term, *personally identifiable information*, did not include IP addresses, which identify a computer rather than a person. In the words of the court, "[i]n order for 'personally identifiable information' to be personally identifiable, it must identify a person." *Johnson v. Microsoft Corp.,* No. C06-0900 RAJ, 2009 WL 1794400, at *4 (W.D. Wash. June 23, 2009).

[232]*See generally infra* § 27.07 (analyzing putative security breach class action suits).

[233]*See Pineda v. Williams-Sonoma Stores, Inc.*, 51 Cal. 4th 524, 120 Cal. Rptr. 3d 531 (2011); Ian C. Ballon & Robert Herrington, Are Your Data Collection Practices Putting Your Company At Risk?, ABA Information Security & Privacy News (Autumn 2011); *see generally supra* § 26.13[6][E] (analyzing the case and underlying statute).

Where litigation is premised on a third party's privacy violation, rather than a direct violation by the defendant, or on a defendant's mere republication of material, the suit may be preempted by the Communications Decency Act.[234] The exemption, however, does not apply, among other things, to the federal Electronic Communications Privacy Act[235] "or any similar State law."[236]

As noted earlier, many putative class action cases settle. Class action settlements typically are structured to provide payments and/or equitable relief, in addition to an award of attorneys' fees to class counsel.[237] While certification of a li-

---

[234]*See* 47 U.S.C.A. § 230(c); *see also, e.g.*, *Carafano v. Metrosplash.com. Inc.*, 339 F.3d 1119, 1125 (9th Cir. 2003) (holding plaintiff's privacy claim preempted); *Collins v. Purdue University*, 703 F. Supp. 2d 862, 877–80 (N.D. Ind. 2010) (false light); *Doe v. Friendfinder Network, Inc.*, 540 F. Supp. 2d 288 (D.N.H. 2008); *Parker v. Google, Inc.*, 422 F. Supp. 2d 492, 500–01 (E.D. Pa. 2006), *aff'd mem.*, 242 F. App'x 833 (3d Cir. 2007), *cert. denied*, 552 U.S. 156 (2008); *Barrett v. Fonorow*, 343 Ill. App. 3d 1184, 279 Ill. Dec. 113, 799 N.E.2d 916 (2d Dist. 2003) (false light invasion of privacy and defamation); *see generally infra* § 37.05 (analyzing the CDA and discussing other cases).

[235]47 U.S.C.A. § 230(e)(4). The Electronic Communications Privacy Act, 18 U.S.C.A. §§ 2510 *et seq.*, is discussed briefly in section 26.09 and more extensively in sections 44.06, 44.07 and 50.06[4] (and briefly in section 58.07[5][A]).

[236]47 U.S.C.A. § 230(e)(4).

[237]*See, e.g.*, *In re Google Referrer Header Privacy Litig.*, 869 F.3d 737 (9th Cir. 2017) (affirming a *cy pres* only settlement and holding that the district court did not abuse its discretion in awarding $2.125 million in attorneys' fees), *cert. granted*, 138 S. Ct. 1697 (2018); *Fraley v. Facebook, Inc.*, 638 F. App'x 594 (9th Cir. 2016) (affirming approval of *cy pres* class action settlement); *Lane v. Facebook, Inc.*, 696 F.3d 811 (9th Cir. 2012) (approving an attorneys' fee award of $2,364,973.58 and a $9.5 million cy pres class action settlement in a suit over Facebook's beacon program brought under the Electronic Communications Privacy Act, Video Privacy Protection Act, Computer Fraud and Abuse Act, the California Consumer Legal Remedies Act, and California Computer Crime Law (Cal. Penal Code § 502), and for remedies for unjust enrichment), *cert. denied*, 134 S. Ct. 8 (2013); *In re Yahoo Mail Litigation*, No. 13-cv-4980-LHK, 2016 WL 4474612 (N.D. Cal. Aug. 25, 2016) (granting final approval of a class action settlement); *Perkins v. LinkedIn Corp.*, Case No. 13-CV-04303-LHK, 2016 WL 613255 (N.D. Cal. Feb. 16, 2016) (granting final approval of a class action settlement); *Berry v. Schulman*, 807 F.3d 600 (4th Cir. 2015) (affirming approval of a FCRA settlement class); *In re LinkedIn User Privacy Litigation*, 309 F.R.D. 573 (N.D. Cal. 2015) (approving a settlement by a class of users who alleged that LinkedIn had failed to adequately protect user information for premium subscribers); *Kim v. Space Pencil, Inc.*, No. C 11-03796 LB, 2012 WL 5948951 (N.D. Cal. Nov.

ability class is usually fought by defendants, once a settlement is reached the parties typically jointly seek court approval for a settlement class, which maximizes the preclusive effect of any settlement. Settlements and fee awards are subject to court approval.[238]

The volume of putative privacy class action suits filed since 2010 underscores that privacy suits, whether or not meritorious, may impose a significant cost on Internet and mobile companies.

Businesses may limit their risk of exposure to class action litigation by users or customers where there is privity of contract by including binding arbitration provisions and class action waivers in consumer contracts. As analyzed at length in section 22.05[2][M], arbitration provisions (including those containing a prohibition on class-wide remedies) are generally enforceable in standard form consumer contracts, including Terms of Use, as a result of the U.S. Supreme Court's 2011 decision in *AT&T Mobility, LLC v. Concepcion*[239] and subsequent case law. Class action waivers in contracts litigated in court, however, may or may not be enforceable, depending on the jurisdiction whose law is applied.[240]

Even without a class action waiver, if the court finds that there is a binding arbitration agreement, the entire case will be stayed and arbitration compelled—effectively preventing

---

28, 2012) (approving settlement of a suit alleging that Kissmetrics surreptitiously tracked plaintiffs' web browsing activities, pursuant to which Kissmetrics had agreed not to use the browser cache, DOM (HTML 5) local storage, Adobe Flash LSOs or eTags to "respawn" or repopulate HTTP cookies and awarding plaintiffs $474,195.49 in attorneys' fees in addition to costs and incentive payments to the named plaintiffs).

Approval for proposed data privacy class action settlements is sometimes denied. *See, e.g.*, *In re Target Corp. Customer Data Security Breach Litig.*, 847 F.3d 608 (8th Cir. 2017) (reversing and remanding class action settlement); *Matera v. Google, Inc.*, Case No. 15-CV-04062-LHK, 2017 WL 1365021 (N.D. Cal. Mar. 15, 2017) (denying preliminary approval to a proposed class action settlement over concerns about the clarity of notice and adequacy of evidence submitted in support of the proposed settlement). Where approval has not been obtained, it may be possible for the parties to modify the terms of the proposed settlement to address a court's concerns, and later obtain approval. *See, e.g.*, *In re Target Corp. Customer Data Security Breach Litigation*, 892 F.3d 968 (8th Cir. 2018) (affirming final approval of a class action settlement, following remand).

[238]*See supra* § 25.07[2].

[239]*AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011).

[240]*See supra* § 22.05[2][M].

plaintiffs' counsel from even moving for class certification.[241] Judges, however, closely scrutinize unilateral contracts with consumers and will not enforce arbitration provisions if assent to the proposed agreement has not been obtained[242] or if the agreement is unconscionable. A court, however, may not find an agreement unconscionable merely because it would deprive a plaintiff of the ability to seek class-wide relief.[243]

The law governing arbitration agreements and class action waivers in unilateral contracts is analyzed in section 22.05[2][M] and chapter 56. How to draft an arbitration provision to maximize its enforceability is separately considered in section 22.05[2][M][vi].

Like patent troll and stock drop cases, data privacy suits may be viewed as a cost of doing business in today's digital economy. Whether and how a company responds to these suits may determine how many more get brought against it by class action lawyers down the road.

---

[241]*See, e.g.*, *Meyer v. Uber Technologies, Inc.*, 868 F.3d 66 (2d Cir. 2017) (enforcing an online arbitration agreement where the company provided reasonable notice of the terms and the consumer manifested assent); *Tompkins v. 23andMe, Inc.*, 840 F.3d 1016, 1033 (9th Cir. 2016) (enforcing an arbitration provision in 23andMe's Terms of Service agreement as not unconscionable); *Pincaro v. Glassdoor, Inc.*, 16 Civ. 6870 (ER), 2017 WL 4046317 (S.D.N.Y. Sept. 12, 2017) (compelling arbitration of a putative security breach class action suit); *In re RealNetworks, Inc. Privacy Litig.*, Civil No. 00 C 1366, 2000 WL 631341 (N.D. Ill. May 8, 2000) (denying an intervenor's motion for class certification where the court found that RealNetworks had entered into a contract with putative class members that provided for binding arbitration); *see generally supra* § 22.05[2][M] (analyzing the issue and discussing more recent case law).

[242]*See, e.g.*, *Specht v. Netscape Communications Corp.*, 306 F.3d 17 (2d Cir. 2002) (declining to enforce an arbitration provision contained in posted terms accessible via a link and holding such terms to not be binding on users because assent was not obtained); *see generally supra* §§ 21.03 (analyzing online contract formation), 22.05[2][M] (arbitration provisions in unilateral consumer contracts).

[243]*See AT&T Mobility LLC v. Concepcion*, 563 U.S. 333 (2011); *supra* § 22.05[2][M].

E-COMMERCE & INTERNET LAW: TREATISE WITH FORMS 2D 2019

Ian C. Ballon

NEW AND IMPORTANT FEATURES FOR 2019 NOT FOUND ELSEWHERE

The Preeminent Internet and Mobile Law Treatise from a leading Internet litigator — now a 5 volume set!

To order call **1-888-728-7677**
or visit **legalsolutions.thomsonreuters.com**

Key Features of E-Commerce & Internet Law

- The California Consumer Privacy Act, GDPR, California IoT security statute, Vermont data broker registration law, Ohio safe harbor statute and other important privacy and cybersecurity laws
- Understanding conflicting law on mobile contract formation, unconscionability and enforcement of arbitration and class action waiver clauses
- The most comprehensive analysis of the TCPA's application to text messaging and its impact on litigation found anywhere
- Complete analysis of the Cybersecurity Information Sharing Act (CISA), state security breach statutes and regulations, and Defend Trade Secrets Act (DTSA) and their impact on screen scraping and database protection, cybersecurity information sharing and trade secret protection, privacy obligations and the impact that Terms of Use and other internet and mobile contracts may have in limiting the broad exemption from liability otherwise available under CISA
- Comprehensive and comparative analysis of the platform liability of Internet, mobile and cloud site owners, and service providers, for user content and misconduct under state and federal law
- Understanding the laws governing SEO and SEM and their impact on e-commerce vendors, including major developments involving internet advertising and embedded and sponsored links
- AI, screen scraping and database protection
- Strategies for defending cybersecurity breach and data privacy class action suits
- Copyright and Lanham Act fair use, patentable subject matter, combating genericide, right of publicity laws governing the use of a person's images and attributes, initial interest confusion, software copyrightability, damages in internet and mobile cases, the use of icons in mobile marketing, new rules governing fee awards, and the applicability and scope of federal and state safe harbors and exemptions
- How to enforce judgments against foreign domain name registrants
- Valuing domain name registrations from sales data
- Compelling the disclosure of the identity of anonymous and pseudonymous tortfeasors and infringers
- Exhaustive statutory and case law analysis of the Digital Millennium Copyright Act, the Communications Decency Act (including exclusions created by FOSTA-SESTA), the Video Privacy Protection Act, and Illinois Biometric Privacy Act
- Analysis of the CLOUD Act, BOTS Act, SPEECH Act, Consumer Review Fairness Act, N.J. Truth-in-Consumer Contract, Warranty and Notice Act, Family Movie Act and more
- Practical tips, checklists and forms that go beyond the typical legal treatise
- Clear, concise, and practical analysis

AN ESSENTIAL RESOURCE FOR ANY INTERNET AND MOBILE, INTELLECTUAL PROPERTY OR DATA PRIVACY/ CYBERSECURITY PRACTICE

E-Commerce & Internet Law is a comprehensive, authoritative work covering law, legal analysis, regulatory issues, emerging trends, and practical strategies. It includes practice tips and forms, nearly 10,000 detailed footnotes, and references to hundreds of unpublished court decisions, many of which are not available elsewhere. Its unique organization facilitates finding quick answers to your questions.

The updated new edition offers an unparalleled reference and practical resource. Organized into five sectioned volumes, the 59 chapters cover:

- Sources of Internet Law and Practice
- Intellectual Property
- Licenses and Contracts
- Data Privacy, Cybersecurity and Advertising
- The Conduct and Regulation of E-Commerce
- Internet Speech, Defamation, Online Torts and the Good Samaritan Exemption
- Obscenity, Pornography, Adult Entertainment and the Protection of Children
- Theft of Digital Information and Related Internet Crimes
- Platform liability for Internet Sites and Services (Including Social Networks, Blogs and Cloud services)
- Civil Jurisdiction and Litigation

Distinguishing Features

- Clear, well written and with a practical perspective based on how issues actually play out in court (not available anywhere else)
- Exhaustive analysis of circuit splits and changes in the law combined with a common sense, practical approach for resolving legal issues, doing deals, documenting transactions and litigating and winning disputes
- Covers laws specific to the Internet and explains how the laws of the physical world apply to internet and mobile transactions and liability risks
- Addresses both law and best practices
- Comprehensive treatment of intellectual property, data privacy and mobile and Internet security breach law

SUMMARY OF CONTENTS

"Should be on the desk of every lawyer who deals with cutting edge legal issues involving computers or the Internet."
Jay Monahan
General Counsel, ResearchGate

****
ABOUT THE AUTHOR
****

IAN C. BALLON

Ian Ballon is Co-Chair of Greenberg Traurig LLP's Global Intellectual Property and Technology Practice Group and is a litigator based in the firm's Silicon Valley and Los Angeles offices. He defends data privacy, cybersecurity breach, TCPA, and other Internet and mobile class action suits and litigates copyright, trademark, patent, trade secret, right of publicity, database and other intellectual property matters, including disputes involving Internet-related safe harbors and exemptions and platform liability.

Mr. Ballon was the recipient of the 2010 Vanguard Award from the State Bar of California's Intellectual Property Law Section. He also has been recognized by *The Los Angeles and San Francisco Daily Journal* as one of the Top 75 Intellectual Property litigators, Top Cybersecurity and Artificial Intelligence (AI) lawyers, and Top 100 lawyers in California.

In 2017 Mr. Ballon was named a "Groundbreaker" by *The Recorder* at its 2017 Bay Area Litigation Departments of the Year awards ceremony and was selected as an "Intellectual Property Trailblazer" by the *National Law Journal*.

Mr. Ballon was named as the Lawyer of the Year for information technology law in the 2019, 2018, 2016 and 2013 editions of *The Best Lawyers in America* and is listed in Legal 500 U.S., The Best Lawyers in America (in the areas of information technology and intellectual property) and Chambers and Partners USA Guide in the areas of privacy and data security and information technology. He also serves as Executive Director of Stanford University Law School's Center for E-Commerce in Palo Alto.

Mr. Ballon received his B.A. *magna cum laude* from Tufts University, his J.D. *with honors* from George Washington University Law School and an LLM in international and comparative law from Georgetown University Law Center. He also holds the C.I.P.P./U.S. certification from the International Association of Privacy Professionals (IAPP).

In addition to *E-Commerce and Internet Law: Treatise with Forms 2d edition*, Mr. Ballon is the author of *The Complete CAN-SPAM Act Handbook* (West 2008) and *The Complete State Security Breach Notification Compliance Handbook* (West 2009), published by Thomson West (www.IanBallon.net).

He may be contacted at BALLON@GTLAW.COM and followed on Twitter and LinkedIn (@IanBallon).

Contributing authors: Parry Aftab, Ed Chansky, Francoise Gilbert, Tucker McCrady, Josh Raskin, Tom Smedinghoff and Emilio Varanini.

NEW AND IMPORTANT FEATURES FOR 2019

- A comprehensive analysis of the **California Consumer Information Privacy Act**, **California's Internet of Things (IoT) security statute**, **Vermont's data broker registration law**, **Ohio's safe harbor** for companies with written information security programs, and other new state laws governing cybersecurity (chapter 27) and data privacy (chapter 26)
- An exhaustive analysis of **FOSTA-SESTA** and what companies should do to maximize CDA protection in light of these new laws (chapter 37)
- The **CLOUD Act** (chapter 50)
- Understanding **the TCPA after *ACA Int'l*** and significant new cases & circuit splits (chapter 29)
- Fully updated **50-state compendium** of security breach notification laws, with a **strategic approach** to handling notice to consumers and state agencies (chapter 27)
- **Platform liability and statutory exemptions and immunities** (including a comparison of "but for" liability under the CDA and DMCA, and the latest law on secondary trademark and patent liability) (chapter 49)
- Applying **the single publication rule** to websites, links and uses on social media (chapter 37)
- The complex array of potential liability risks from, and remedies for, **screen scraping, database protection and use of AI to gather data and information online** (chapter 5)
- State online dating and revenge porn laws (chapter 51)
- **Circuit splits on Article III standing in cybersecurity litigation** (chapter 27)
- Revisiting **sponsored link, SEO and SEM practices and liability** (chapter 9)
- **Website and mobile accessibility** (chapter 48)
- **The Music Modernization Act's Impact on copyright preemption and DMCA protection for pre-1972 musical works** (chapter 4)
- **Compelling the disclosure of passwords and biometric information to unlock a mobile phone, tablet or storage device** (chapter 50)
- Cutting through the jargon to make sense of ***clickwrap*, *browsewrap*, *scrollwrap* and *sign-in wrap* agreements (and what many courts and lawyers get wrong about online contract formation)** (chapter 21)
- The latest case law, trends and strategy for **defending cybersecurity and data privacy class action suits** (chapters 25, 26, 27)
- **Click fraud** (chapter 28)
- Updated **Defend Trade Secrets Act** and UTSA case law (chapter 10)
- **Drafting enforceable arbitration clauses and class action waivers** (with new sample provisions) (chapter 22)
- **Applying the First Sale Doctrine to the sale of digital goods and information** (chapter 16)
- **The GDPR, ePrivacy Directive and transferring data from the EU/EEA** (by Francoise Gilbert) (chapter 26)
- **Patent law** (updated by Josh Raskin) (chapter 8)
- **Music licensing** (updated by Tucker McCrady) (chapter 17)
- **Mobile, Internet and Social Media contests & promotions** (updated by Ed Chansky) (chapter 28)
- **Conducting a risk assessment and creating a Written Information Security Assessment Plan (WISP)** (by Thomas J. Smedinghoff) (chapter 27)